

EXHIBIT 1

BOIES SCHILLER FLEXNER LLP

David Boies (admitted pro hac vice)
333 Main Street
Armonk, NY 10504
Tel: (914) 749-8200
dboies@bsfllp.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No.
238027
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted pro hac vice)
Rossana Baeza (admitted pro hac vice)
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsfllp.com
rbaeza@bsfllp.com

Alison L. Anderson, CA Bar No. 275334
M. Logan Wright
725 S Figueroa St., 31st Floor
Los Angeles, CA 90017
Tel.: (213) 995-5720
alanderson@bsfllp.com
mwright@bsfllp.com

SUSMAN GODFREY L.L.P.

Bill Carmody (admitted pro hac vice)
Shawn J. Rabin (admitted pro hac vice)
Steven M. Shepard (admitted pro hac vice)
Alexander Frawley (admitted pro hac vice)
Ryan Sila (admitted pro hac vice)
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel.: (212) 336-8330
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@susmangodfrey.com
rsila@susmangodfrey.com

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel.: (310) 789-3100
abonn@susmangodfrey.com

MORGAN & MORGAN

John A. Yanchunis (admitted pro hac vice)
Ryan J. McGee (admitted pro hac vice)
Michael F. Ram, CA Bar No. 104805
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com
mram@forthepeople.com

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

ANIBAL RODRIGUEZ, SAL CATALDO,
JULIAN SANTIAGO, and SUSAN LYNN
HARVEY individually and on behalf of all
other similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No.: 3:20-cv-04688-RS

**DECLARATION OF BRUCE SCHNEIER
IN SUPPORT OF PLAINTIFFS'
MOTION FOR CLASS CERTIFICATION**

Judge: Hon. Richard Seeborg
Courtroom 3 – 17th Floor
Date: October 5, 2023
Time: 1:30 p.m.

DECLARATION OF BRUCE SCHNEIER

I, Bruce Schneier, declare as follows.

1. Counsel for the *Rodriguez* Plaintiffs retained me to provide expert analysis and, if requested, expert testimony. I have personal knowledge of the matters set forth herein and am competent to testify.

2. I submit this declaration in connection with Plaintiffs' Motion for Class Certification.

3. Attached is a true and correct copy of the Expert Report that I prepared in connection with this matter, dated February 20, 2023. The opinions I provided therein are true and correct to the best of my knowledge.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 17th day of July, 2023, at Cambridge, MA.

/s/  _____

Rodriguez v. Google

I. Introduction.....	4
II. Background	4
III. Expertise	5
IV. Data and Privacy Topics	7
1. <i>Privacy</i>	7
1.1. “Privacy” Has a Specific Meaning and Implications.....	7
1.2. Privacy Is a Basic Human Need.....	8
1.3. Privacy Is Crucial for Political Liberty and Justice	9
1.4. Privacy Is Crucial for People’s Business and Personal Relationships	10
1.5. Problems Arise when Businesses Disregard Privacy	11
2. <i>Data Privacy</i>	12
2.1. Privacy Has Become a Significant Issue with the Rise of the Internet	12
2.2. Surveillance Is the Primary Business Model of the Internet.....	14
2.3. Privacy Has Become More Important with Widespread Corporate Surveillance	17
3. <i>User Data</i>	18
3.1. Personal Data Is a Byproduct of Computing	18
3.2. User Data Encompasses Many Things, Including Data Generated by User Activities.....	22
3.3. Information from App Activity Is Highly Personal	23
3.4. Information about Online Activity Is Unique for Each User	25
3.5. Online Advertising Has Risks for Users	26
3.6. User Activity on Mobile Apps Is Sensitive Information.....	27
4. <i>The Value of User Data</i>	29
4.1. User Data Generates Billions in Corporate Revenue	29
4.2. Third Parties Perform Electronic Tracking.....	33
5. <i>Limitations on Collecting User Data</i>	34
5.1. Laws Impose Restrictions on How Companies Can Collect Data	34
5.2. Restrictions Focus on Collection as Well as Saving and Use	35
5.3. There Are Many Privacy Risks Post-Collection	38
6. <i>Privacy and System Design</i>	39
6.1. People’s Privacy Intuition Is Not Suited for the Internet.....	39
6.2. Personal Data Is Difficult to Anonymize and Easy to De-anonymize	41
6.3. The Industry Uses Dark Patterns to Nudge Users in Particular Directions.....	44
V. Google-Specific Topics.....	52
7. <i>Google’s Surveillance-Dependent Business Model</i>	52
7.1. Google Makes Money from Harvesting User Data.....	52
7.2. Google Search Has an Overwhelming Market Share.....	55
7.3. Google’s Android OS Dominates the Global Smartphone Market.....	58
7.4. It Is Practically Impossible to Avoid Using Google Products and Services	60
7.5. Google Collects Data About Users’ Interactions with Non-Google Websites and Apps	61
8. <i>User Risks Caused by Google’s Data Collection</i>	63
8.1. Users Face Risks from Joinability of Disparate Google Data Sets	63
8.2. Google Has a History of Data Breaches	65
8.3. Google Has a History of Privacy and Consent Failures.....	67
9. <i>User Control over Google Tracking and Collection</i>	72
9.1. Google Promises Users Control over the Company’s Collection of Their Data.....	72

Rodriguez v. Google

9.2.	Giving Users Privacy Control Is Important for Google’s Brand, and Getting/Keeping Users	74
9.3.	Google’s Notice and Consent Procedures Are Confusing	77
9.4.	Google Uses Dark Patterns	80
VI.	Google Tracking and Web & App Activity Topics	85
10.	<i>WAA and User Control</i>	85
10.1.	Google Presented WAA and sWAA as Ways for Users to Control Their Privacy	85
10.2.	Anonymization Does Not Protect the Privacy of WAA and sWAA Data	87
11.	<i>Google’s Use of Dark Patterns</i>	88
11.1.	Google’s WAA Help Page Exemplifies Dark Patterns	88
11.2.	Disclosures Accompanying the WAA and sWAA Toggles, including the “Activity Controls” Page, Exemplify Dark Patterns.....	92
11.3.	Google Statements about Privacy and User Control Exemplify Dark Patterns	94
11.4.	Google’s WAA Controls for Location Privacy Exemplify Dark Patterns	99
11.5.	Google’s WAA/sWAA “Consent Bump” Prompt Exemplifies Dark Patterns	100
11.6.	Google’s Disclosures to App Developers Exemplify Dark Patterns.....	103
11.7.	Google Employees Repeatedly Identified Problems with Google’s Disclosures Regarding WAA/sWAA, but Google Ignored Them	105
11.8.	Google Uses Dark Patterns to Manipulate User Behavior to Its Own Benefit	108

I. Introduction

1. The rise of the Internet and surveillance business models have increased threats to privacy, making it more important than ever for users to have a refuge from pervasive tracking. The rise of mobile devices exacerbates the privacy threats associated with the Internet more generally; data collected from mobile devices is especially sensitive since users generally carry them wherever they go. The volume and scope of data generated reveals sensitive information about individual users, which is highly valuable to commercial actors. These commercial actors have an economic interest in fabricating the appearance of consent, and easily manipulate users' expectations. Accordingly, effective protection of privacy requires disclosures and controls not just in terms of how data is used but of what data is collected in the first place. Anonymization tactics are insufficient. It is easy to associate data with users, particularly where the data is explicitly tied to device identifiers.

2. Google is one of those commercial actors; it has overwhelming incentives to maximize collection of data about users and it has unmatched power to do so. Case-in-point is Google's collection of data about users' activity on non-Google apps by way of Google services like Google Analytics for Firebase, Ad Mob, and Ad Manager. Google has constructed an essentially inescapable infrastructure for gathering a vast scope of information about users' activity on non-Google apps.

3. Google fails to adequately disclose or provide notice of its data collection practices or to provide users with effective privacy controls. Google fails to adequately disclose or provide notice of its data collection practices or to provide users with effective privacy controls. Google brands and positions itself as a privacy-conscious organization, but the Google "privacy controls" addressed in this lawsuit (Web & App Activity (WAA) and Supplemental Web & App Activity (sWAA)) are merely an illusion. Contrary to how Google describes them to both users and app developers, WAA and sWAA do not prevent Google from collecting, saving, and using account holders' app activity. These settings also do not prevent Google from collecting, saving, and using that data in connection with persistent, Google-created and -controlled identifiers like AdID. Instead, Google's uses dark patterns—subversive user interface designs that manipulate users into making decisions that serve Google's purposes rather than their own—to provide users and app developers with a false sense of security that Google respects users' privacy choices. Although Google portrays itself as a champion of user privacy, Google's incentives and actions lead me to believe that it is more concerned with managing user impressions than actually respecting user privacy.

II. Background

4. Counsel for the Plaintiffs in this action ("Counsel") retained me to develop and provide opinions concerning issues of privacy and the alleged conduct, as detailed in this report. My analysis included issues relating to Google's disclosures and practices, the WAA and sWAA controls at issue, and issues relating to the value of privacy and user data.

Rodriguez v. Google

5. I am compensated at the rate of \$825/hour and my research associate, Kathleen Seidel, is compensated at the rate of \$125/hour. Our compensation does not depend upon the outcome of the case. In the event of any recovery in this case, I understand that Ms. Seidel and I will be excluded from any disbursement of funds.

6. In preparing my report I have considered the documents identified herein, as well as those documents which are listed in Appendix 1. As part of my research, Ms. Seidel and I had access to a database containing over 26,000 documents that Google produced during the discovery process in this case and marked “Confidential.” We were not provided access to documents designated “Highly Confidential—Attorneys’ Eyes Only.” Ms. Seidel and I used the ILS document review platform to search for relevant documents. We had free range to conduct our own searches within this database of “Confidential” documents. We also had access to Google’s Interrogatory and Request for Admission responses, except for any materials marked as “Highly Confidential—Attorneys’ Eyes Only.” Finally, we had access to all deposition transcripts for depositions of Google employees as well as for all of the named plaintiffs’ deposition transcripts.

7. This report has been prepared for purposes of this case only. It may not be used for any other purpose. This report contains and refers to information designated as “Confidential” under a Stipulated Protective Order, to which Ms. Seidel and I have agreed to be bound. I have not reviewed or relied on any discovery produced by Google marked as “Highly Confidential—Attorneys’ Eyes Only.” Those were not accessible to me.

III. Expertise

8. My name is Bruce Schneier. I hold an MS Degree in Computer Science, which I obtained from American University in 1986, and a BS Degree in Physics, which I obtained from the University of Rochester in 1984.

9. I work internationally as a security technologist. I presently hold the title of Chief of Security Architecture at Inrupt, Inc. From 2016 until 2019, I held the titles of Chief Technology Officer of Resilient Systems, Inc., then Special Advisor to IBM Security. Prior to that, from 1999 until 2016, I was Chief Technology Officer of Counterpane Internet Security, Inc., and Chief Security Technology Officer of BT. I am also the President of Counterpane Systems LLC, and have been since 1991.

10. I am an Adjunct Lecturer and fellow at the Harvard Kennedy School, where I teach cybersecurity policy. My Spring survey course is “Cybersecurity: Tech, Policy, and Law.” My Fall seminar module is “Special Topics in Cybersecurity Policy.” Past topics have included AI security, blockchain, election security, and misinformation.

11. I am associated with the Belfer Center for Science and International Affairs, and the Ash Center for Democracy and Technology—where I have an office—both at the Harvard Kennedy School. I am also a fellow at the Berkman Klein Center for Internet and Society at Harvard University.

12. I serve as board member of the Electronic Frontier Foundation and Access Now. I have formerly been a board member of the Electronic Privacy Information Center and the Tor Project.

Rodriguez v. Google

I serve as an advisory board member for the Electronic Privacy Information Center, Verified Voting, and Sightline Security.

13. I am the author of approximately twelve books on the topics of cryptography, computer security, general security technology, trust, surveillance, and privacy, including *Applied Cryptography* (1994 and 1996), *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (2003), *Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World* (2015), and *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (2018). My new book, *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back*, was published by W.W. Norton in February 2023.

14. My work entails the technical aspects of cryptography, computer security, and Internet security. I also research, write, and speak about the economic, psychological, and sociological aspects of security and privacy. As such, I study user behavior and human factors related to many different aspects of security and privacy. My 2014 book, *Data and Goliath*, discusses people's relationship with privacy, and their behaviors regarding privacy, in detail. *A Hacker's Mind* discusses dark patterns.

15. I have also authored or coauthored over 100 academic publications on security technology subjects, such as cryptographic design and analysis, security protocol design and analysis, software security, information security, Internet security, security technologies, data privacy, data anonymity, AI security, security policy, privacy policy, cyberespionage, and cyberwarfare.

16. I have published numerous articles on the subject of security technology and its effects at personal, corporate, and national levels, for publications such as the *New York Times*, the *Washington Post*, the *Wall Street Journal*, the *Guardian*, *Atlantic*, *Foreign Policy*, *Forbes*, *Wired*, *Nature*, the *Sydney Morning Herald*, the *Boston Globe*, and the *San Francisco Chronicle*. I have repeatedly testified before Congress on these topics.

17. I regularly speak at security conferences around the world.

18. I am the recipient of many awards, including: (1) Electronic Privacy Information Center Lifetime Achievement Award, 2015; (2) named one of the IFSEC 40: The Most Influential People in Security & Fire, January 2013; (3) Honorary Doctor of Science (ScD) from University of Westminster, London, December 2011; (4) CSO Compass Award, May 2010; (5) Computer Professionals for Social Responsibility (CPSR) Norbert Weiner Award, January 2008; (6) Electronic Frontier Foundation (EFF) Pioneer Award, March 2007; (7) *Dr. Dobb's Journal* Excellence in Programming Award, April 2006; (8) *InfoWorld* CTO 25 Award, April 2005; and (9) Productivity Award for *Secrets and Lies* in the 13th Annual *Software Development Magazine* Product Excellence Awards, 2000.

19. I am the author of a monthly email newsletter about security, "Crypto-Gram," and the blog "Schneier on Security," which have a combined readership of over 250,000 people.

20. I am a named co-inventor on eighty-two issued US Patents relating to cryptography, computer security, security technology, and electronic commerce.

Rodriguez v. Google

21. Yes, I also find time to sleep.¹

22. I have spent my entire career focused on issues relating to digital privacy. Before Counsel contacted me about being retained as an expert in this litigation, I was familiar with Internet privacy controls in general but was unaware of the details of the conduct at issue in this litigation: that is, Google’s collection and storage of detailed information about people who use non-Google mobile apps with their WAA and sWAA controls turned off. It was only through my access to Confidential discovery in this litigation that I understood the extent of these Google practices.

23. My detailed CV is included as Appendix 2 to this report. That CV lists declarations and depositions I have given as an expert witness in previous court cases.

IV. Data and Privacy Topics

1. Privacy

1.1. “Privacy” Has a Specific Meaning and Implications

24. I understand that this case involves Google’s collection, storage, and use of information from users of mobile apps who have turned off WAA and/or sWAA.

25. I also understand from Counsel that, for some of the legal claims that Plaintiffs are bringing, Plaintiffs seek to establish that they have a reasonable expectation of privacy regarding their use of mobile apps and that Google’s collection and use of mobile app data from users who have turned off WAA and sWAA is highly offensive to a reasonable user.

26. To provide context for these issues, it is important to begin with a more general overview of data privacy in the context of Internet usage. As I will describe below, people are persistently tracked in today’s Internet age, making it all the more important for people to have a refuge from this surveillance. Google has portrayed its privacy controls, namely WAA and sWAA, as that refuge. Unfortunately for users, Google made and then reneged on its promise not to collect, save, or use users’ mobile app data if those users turned off WAA or sWAA.

27. According to the Oxford English Dictionary, the word “privacy” dates back to the 1500s, and refers to “The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.” Privacy consists of freedom from attention by those one can see, and by those one cannot see. With respect to communication, the OED defines “private” as “intended only for or confined to the person or persons directly concerned; confidential.”²

28. When labeling products as “privacy settings” or “privacy controls,” common practice is to assume that user expectations will include the broadest scope of such words.

¹ Pretty well; thanks for asking.

² *Oxford English Dictionary Online*, “Private” (retrieved February 20, 2023).

Rodriguez v. Google

29. Privacy is linked to the concept of control. The National Institute of Standards and Technology defines “privacy” as “assurance that the confidentiality of, and access to, certain information about an entity is protected; the right of a party to maintain control over and confidentiality of information about itself; freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.”³

1.2. Privacy Is a Basic Human Need

30. Privacy is central to our ability to control how we relate to the world. Being stripped of privacy is fundamentally dehumanizing, whether it is conducted by an undercover police officer following us around or by computer algorithms and systems tracking our online activities.

31. There is a strong physiological basis for privacy. Biologist Peter Watts makes the point that a desire for privacy is innate: mammals in particular don’t respond well to surveillance. Humans consider surveillance a physical threat, as do animals in the natural world who are stalked by predators. Surveillance—defined by the US military as “systematic observation”⁴—makes people feel like prey, just as it makes the surveillors behave like predators.⁵

32. Based on my experience as a technologist with a special interest not only in the technical aspects of privacy but its social and historical context, and not as a lawyer, I understand that the vision of privacy as a fundamental human right is enshrined in both US and international law. It is my understanding as a security and privacy professional that the right to privacy is implied in the Fourth, Fifth, and Ninth Amendments of the US Constitution,⁶ and that it is enumerated in the Universal Declaration of Human Rights (1948),⁷ the European Convention on Human Rights (1970),⁸ and the 2000 Charter of Fundamental Rights of the European Union.⁹ I understand that privacy is also a right enshrined in California’s Constitution.¹⁰

³ National Institute of Standards and Technology, Computer Security Resource Center, “Glossary,” <https://csrc.nist.gov/glossary/term/privacy> (accessed February 20, 2023).

⁴ US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> (November 2021).

⁵ Peter Watts, “The scorched earth society,” Symposium of the International Association of Privacy Professionals, Toronto, Ontario, <https://rifiers.com/real/shorts/TheScorchedEarthSociety-transcript.pdf> (May 9, 2014).

⁶ FindLaw, “Is there a ‘right to privacy’ amendment?” <https://www.findlaw.com/injury/torts-and-personal-injuries/is-there-a-right-to-privacy-amendment.html> (September 30, 2019).

⁷ United Nations, “Universal Declaration of Human Rights,” <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (December 10, 1948) (“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence”).

⁸ Council of Europe, “European Convention on Human Rights,” https://www.echr.coe.int/Documents/Convention_ENG.pdf (1953) (“Everyone has the right to respect for his private and family life, his home and his correspondence”).

⁹ European Union, “Charter of Fundamental Rights of The European Union,” https://www.europarl.europa.eu/charter/pdf/text_en.pdf (2000).

¹⁰ Article I, section 1 of the California Constitution provides: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and

Rodriguez v. Google

33. In 2013, the UN General Assembly approved a resolution titled “The right to privacy in the digital age,” affirming that a fundamental right to privacy applies online as well as offline, and that the risk of surveillance undermines this right.¹¹ The right to privacy recognized by all of these sources informs the normative expectation of ethical software designers that privacy should be protected.

34. One 2013 study found that an increase in users’ perceived control over the privacy of their personal information—defined as “40 questions, which varied in intrusiveness about the respondent’s life”—is associated with an increased willingness to disclose such information.¹² The study pertained to privacy and data sharing in general, and is relevant when considering Google’s practice of collecting, saving, and using records of users’ activity, particularly because Google’s Privacy Policy represents (at the start, before getting into the various subparts) that it works hard to “put you in *control*,” that you can “use our services in a variety of ways to manage your privacy,” and that “across our services, you can adjust your privacy settings to *control* what we collect and how your information is used.”¹³

35. Privacy is not a luxury that people value or seek only in times of safety. Instead, privacy is a value to be assiduously preserved. Privacy is essential for liberty, autonomy, and human dignity. Privacy is something to maintain and protect in order for humans to be truly secure. This is something I wrote about extensively in my book *Data and Goliath*.¹⁴

1.3. Privacy Is Crucial for Political Liberty and Justice

36. Google and other technology companies collect and save phenomenal amounts of data, sometimes indefinitely. It would be incredibly dangerous to live in a world without privacy where, for example, everything a citizen said and did could be stored and brought forward as evidence against them in the future, or made available to companies that wished to construct cradle-to-grave dossiers on individual citizens. The seventeenth-century French statesman Cardinal Richelieu recognized this when he said, “Show me six lines written by the most honest man in the world, and I will find enough therein to hang him.” Lavrentiy Beria, head of Joseph Stalin’s secret police, declared, “Show me the man, and I’ll show you the crime.”¹⁵ Both were saying the same thing: if you have gathered enough data about a person, you can find sufficient

protecting property and pursuing and obtaining safety, happiness, and privacy.” California Constitution, “Article 1 Declaration of Rights,” California Legislative Information, https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS§ionNum=SECTION%201.&article=I (Article 1 adopted 1879; Sec. 1 added Nov. 5, 1974, by Proposition 7, Resolution Chapter 90, 1974).

¹¹ United Nations Office of the High Commissioner for Human Rights, “The right to privacy in the digital age,” <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx> (2021).

¹² Laura Brandimarte, Alessandro Acquisti and George Loewenstein, “Misplaced confidences: Privacy and the control paradox,” *Social Psychological and Personality Science* 4, no. 3, <https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf> (May 2013).

¹³ Google, “Privacy policy,” <https://policies.google.com/privacy?hl=en> (December 15, 2022).

¹⁴ Bruce Schneier, *Data and Goliath*, Norton (2015).

¹⁵ Harvey Silverglate, *Three Felonies a Day: How the Feds Target the Innocent*, Encounter Books, <https://archive.org/details/harveya.silverglatethreefeloniesadayhowthefedstargettheinnocentencounterbooks20092> (2011).

Rodriguez v. Google

evidence to make them appear guilty of something, even if they are in fact innocent of wrongdoing.

37. Surveillance leads to self-censorship, which stifles the free exchange of ideas. US Supreme Court Justice Sonia Sotomayor recognized the potential chilling effect of surveillance on society in her concurring opinion in *United States v. Jones*, a 2012 case involving the FBI's installation of a GPS tracker on a defendant's car. Justice Sotomayor wrote: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantity of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"¹⁶

38. Surveillance by private entities is no different. When companies like Google collect and save information about individuals, that activity undermines user privacy and creates risks of surveillance and its ensuing harms. Governments can and do seek access to data collected and saved by Google and other tech companies. Although such demands often pertain to criminal investigations, they may also be made for the purpose of monitoring and stifling political dissent. Before Internet-enabled surveillance became common, J. Edgar Hoover spied on Martin Luther King, Jr., and the FBI's COINTELPRO program spied on nonviolent protesters during the Vietnam War. Ubiquitous digital surveillance makes this unseemly sort of work much easier; consider the revelation in 2015 that for years, AT&T collaborated with the NSA to indiscriminately collect US citizens' communications.¹⁷

1.4. Privacy Is Crucial for People's Business and Personal Relationships

39. Google, as a platform for advertising, routinely discriminates by placing people into various categories to enable its business customers to differentially market goods and services to them on the basis of that categorization. Such discrimination can be problematic.

40. Extensive digital surveillance invites surveillance-based discrimination. A 2014 report by the Obama administration recognized the threat posed by the accumulation and analysis of data on American citizens, noting that "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."¹⁸

41. Widespread adoption of digital surveillance by employers can also contribute to unjust workplace conditions. Call center employees, manufacturing workers, and warehouse and retail

¹⁶ US Supreme Court, "Decision," *United States v. Jones*, Case No. 10-1259, <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=000&invol=10-1259#opinion1> (January 23, 2012).

¹⁷ Julia Angwin, et al., "AT&T helped U.S. spy on internet on a vast scale," *New York Times*, <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html> (August 16, 2015).

¹⁸ US Executive Office of the President, "Big data: Seizing opportunities, preserving values," http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (May 1, 2014).

Rodriguez v. Google

staff are commonly surveilled. For example, Amazon's workplace surveillance includes navigation software, item scanners, wristbands, thermal cameras, security cameras, and recorded footage, all of which keep tabs on the location and performance of warehouse employees and delivery drivers.¹⁹ Although 24/7 monitoring is likely to contribute to the efficiency of a company's operation, it also has contributed to workers' feeling that they have no privacy whatsoever on the job. One recent report alleged that Amazon uses surveillance technology to reduce workers' ability to advocate for improved working conditions, analyzing heat maps with information on team member sentiments to identify and limit the effectiveness of potential union organizers.²⁰

1.5. Problems Arise when Businesses Disregard Privacy

42. Threats to privacy are bad for business. In 1993, the US government first tried to restrict the development and export of products that disclosed and incorporated methods of strong cryptography²¹ (products that happened to include my first book, *Applied Cryptography*).²² Concurrently, it promoted the Clipper Chip, a system of encryption that could be bypassed by the FBI and NSA; the agencies, it was argued, would hold the key needed to extract plaintext from encrypted devices "in escrow," only to be used for authorized purposes.²³ However, the first device to include the chip—an AT&T cell phone—was a bust. Neither business enterprises nor privacy-minded citizens in the US were inclined to lay their money down for a supposedly encrypted device that contained a backdoor. Potential customers outside the United States had backdoor-free alternatives that used strong encryption.²⁴

43. Following the 2013 revelations by Edward Snowden regarding the extent of NSA surveillance of the communications of US and foreign residents,²⁵ many US enterprises suffered a severe public relations backlash, and lost the trust and business of many overseas clients. US cloud companies lost customers while their counterparts in countries such as Switzerland gained

¹⁹ Nandita Bose, "Amazon's surveillance can boost output and possibly limit unions: Study," Reuters, <https://www.reuters.com/article/amazon-com-workers-surveillance/amazons-surveillance-can-boost-output-and-possibly-limit-unions-study-idUSKBN25S3F2> (September 15, 2020).

²⁰ Jay Greene, "Amazon's employee surveillance fuels unionization efforts: 'It's not prison, it's work'," *Washington Post*, <https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions> (December 2, 2021).

²¹ Stephen T. Walker, "Oral testimony by Stephen T. Walker, President, Trusted Information Systems, Inc., for Subcommittee on Economic Policy, Trade and Environment, Committee on Foreign Affairs, US House of Representatives," https://irp.fas.org/congress/1993_hr/931012_walker_oral.htm (October 12, 1993).

²² Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, <https://archive.org/details/appliedcryptogra0000schn> (1994).

²³ Wayne Madsen, "The Clipper controversy," *Information Systems Security* 3, <http://www.sciencedirect.com/science/article/pii/1353485894900973> (November 1994).

²⁴ Matt Blaze, "Key escrow from a safe distance: Looking back at the Clipper Chip," 27th Annual Computer Security Applications Conference, Orlando, Florida, <https://www.mattblaze.org/escrow-acsc11.pdf> (December 5-9, 2011).

²⁵ Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *Washington Post*, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-inbroad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (June 7, 2013).

Rodriguez v. Google

them.²⁶ One 2014 survey of British and Canadian companies found that 25% of those queried were moving their data outside the US, even if it meant decreased performance.²⁷ A 2017 study by Microsoft's Office of Chief Economist found that the revelations of mass surveillance decreased the growth rate of US cloud provider revenues by 11% from 2013 to 2014, and estimated losses to the industry of at least \$18 billion.²⁸

44. Following more recent disclosures of data breaches affecting millions of Facebook users, and exploitation of the social media platform by foreign actors seeking to influence the 2016 election, some companies have stopped placing ads there, and many users have curtailed their Facebook activity.²⁹

2. Data Privacy

2.1. Privacy Has Become a Significant Issue with the Rise of the Internet

45. Since its inception in the late 1960s, the Internet has grown from an auxiliary means of communication for academics and members of the military to the nerve-network of modern society, facilitating private, government, educational and commercial interaction; personal intellectual exploration, interpersonal connection and exchange; remote employment and geographically distributed teamwork. Once a service that many people were happy to do without, engagement on the Internet is now integral to participation in modern society.

46. The Internet's early adopters—"netizens," as they were then called—chatted volubly in virtual spaces like The WELL, CompuServe, and local dial-up bulletin boards. The new frontier of "cyberspace" ran on a model of openness, with limited concern that any writings might be read by others than those involved in the conversations. Computers were supposed free individuals and businesses from tedious record-keeping tasks that could be automated, leaving people with more time and energy to engage in creative pursuits, and in tasks requiring face-to-face interaction.

47. Some, however, saw the dark side of the new information and communication regime. In 1994, my late colleague John Perry Barlow, co-founder of the Electronic Frontier Foundation, helped to raise the alarm against the above-described push by US intelligence agencies to require

²⁶ David Gilbert, "Companies turn to Switzerland for cloud storage following NSA spying revelations," *International Business Times*, <http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613> (July 4, 2013).

²⁷ Ellen Messmer, "NSA scandal spooking IT pros in UK, Canada," *Network World*, <http://www.networkworld.com/article/2173190/security/nsa-scandal-spooking-it-pros-in-uk-canada.html> (January 8, 2014).

²⁸ Hyojin Song and Simon Wilkie, "The price of privacy in the cloud: The economic consequences of Mr. Snowden." Microsoft Corporation. https://dornsife.usc.edu/assets/sites/586/docs/song_wilkie_2017.pdf (February 2017).

²⁹ Salvador Rodriguez, "Some advertisers are quitting Facebook, chiding the company's 'despicable business model'," CNBC, <https://www.cnbc.com/2019/03/06/some-advertisers-are-quitting-facebook-after-privacy-scandals.html> (March 6, 2019).

Alex Hern, "Facebook usage falling after privacy scandals, data suggests." *The Guardian*, <https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows> (June 20, 2019).

Rodriguez v. Google

installation of the Clipper chip encryption device in all phones and computers, with the key held by those agencies in the event that they felt the need to intercept and eavesdrop on citizens' communications. In an article in *Wired* magazine, Barlow warned that "the most liberating development in the history of humankind could become, instead, the surveillance system which will monitor our grandchildren's morality. We can be better ancestors than that."³⁰

48. The next twenty-odd years saw the Internet evolve from:

- the era of dial-up bulletin boards and Usenet;
- to the nascent World Wide Web with its hand-crafted HTML, static web pages with little to no advertising save for the occasional banner ad, and few enough websites that the best could be catalogued by hand;
- to the age of blogging, whereby average citizens with little technical skill could set up a website and broadcast their opinions to the world;
- to the new epoch of commercial websites, online stores, and purveyors of entertainment;
- to the era of dynamic databases serving up content and advertising to visitors worldwide;
- to the boom in data-scraping, whereby companies and individuals gathered up publicly available information about individuals, which they then categorized and sold to the highest bidder;
- to the advent of social media sites and apps such as Myspace and Facebook, where users publicly catalogue their friends, their interests, and their photographs;
- to the growth of an advertising ecosystem that homes in on users based on their personal characteristics, and relies upon and profits from the collection, storage, and exploitation of data from and about those users, derived from their activity on online services and products they use.

49. In the forty years since its inception, the Internet has evolved from a specialized means of communication accessible to only a few, to a general communications system that any private citizen with a computer or phone can access, then to a nearly-essential element of everyday life that lives in our pockets and follows us everywhere.

50. "Surveillance" is a politically and emotionally loaded term, in spite of its simple definition as "systematic observation." Modern-day electronic surveillance is exactly that. Private citizens are treated as open books to both governments and corporations; their ability to peer into and analyze our personal lives is greater than it has ever been before.

51. Today's technology enables mass surveillance, and mass surveillance is dangerous. It enables discrimination based on almost any criterion: race, religion, class, or political beliefs, for example. It is being used to control what one sees, what one can do, and, ultimately, what one can say. It is being accomplished without any meaningful checks and balances to level the playing field between individuals and the multinational corporations that control the increasingly complex structure of the Internet. Surveillance makes us less safe and less free. The rules previously established to protect citizens from the dangers of surveillance under earlier technological regimes are now woefully insufficient.

³⁰ John Perry Barlow, "Jackboots on the Infobahn," *Wired*, <https://www.wired.com/1994/04/privacy-barlow> (April 1, 1994).

Rodriguez v. Google

52. The development of the Internet has been liberating for humanity, enabling individuals to access extraordinary amounts of information; connect with others to share their experiences, opinions and concerns; engage in gainful employment (an increasingly important function during the COVID-19 pandemic); and find an appreciative audience for their cat videos. It is also a surveillor's dream. In a 2012 interview, Barlow clarified that both light and dark could and do coincide: "The Internet is the most liberating tool for humanity ever invented, and also the best for surveillance. It's not one or the other. It's both."³¹ In my 2015 book, *Data and Goliath*, I explored at length the competing demands for surveillance and privacy that have emerged in the two decades that followed Barlow's prescient statement; I echo some of the language and many of the sentiments expressed in that book in the remarks that follow here.³²

2.2. Surveillance Is the Primary Business Model of the Internet

53. Surveillance has become the prevailing business model of the Internet for two primary reasons. One: people like things they perceive as free. And two: people like convenient. The truth is, though, that people aren't given a choice between free/convenient products and services that come with surveillance or expensive and/or inconvenient products and services that do not. Even products and services that aren't free include surveillance. For the most part, it's either surveillance or nothing, and the surveillance is often invisible, undisclosed and nonconsensual.

54. Before 1993, the Internet was noncommercial. "Free" became the online norm. When online commercial services first emerged on the Internet, there was a lot of talk about how to charge for them. It quickly became clear that, with some limited exceptions, people at the time were unwilling to pay even a small amount for access. Much like the business model for television, online enterprises turned to advertising as a revenue model, and that revenue model grew phenomenally profitable for those who engaged in surveillance of their users. Advertising platforms can and do charge higher prices for personally targeted advertising than for generally broadcast advertising. Advertising platforms also charge higher prices for advertisements because they can measure the impact of those advertisements on user behavior, a process called conversion tracking. This is how the Internet ended up with a plethora of nominally free websites and mobile apps that collect and sell users' data in exchange for services, then inundate them with advertising.

55. The ordinary bargain that users repeatedly enter into with tech companies (when they do not use privacy controls that promise otherwise, like the WAA and sWAA controls) is surveillance in exchange for nominally free services. In 2013, Google's chairman Eric Schmidt and director of ideas Jared Cohen laid out their vision in *The New Digital Age*.³³ To paraphrase their basic message: if you let us have all your data, we will show you advertisements you want to see and we'll throw in web search, email, calendar, navigation, data storage, and all sorts of other services, at no cost to you. It's all very convenient, and seems to come at little cost. This is the bargain that is often described as: "If you're not paying, then you are the product and not the

³¹ James Ball (April 20, 2012), "Hacktivists in the frontline battle for the internet," *The Guardian*, <https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet> (April 20, 2012).

³² Bruce Schneier, *Data and Goliath*, Norton, <https://archive.org/details/datagoliathhidde0000schn> (2015).

³³ Eric Schmidt and Jared Cohen, *The New Digital Age*, Knopf, https://archive.org/details/newdigitalageres0000schm_w0t9 (2013).

Rodriguez v. Google

customer.” To Google, the attention of its users is the product to be sold to the company’s actual customers: advertisers.

56. Data privacy is at the heart of public discussions of the rise of “surveillance capitalism.” This term was coined by Shoshana Zuboff, professor of psychology at Harvard University, to describe a system that “unilaterally claims human experience as free raw material for translation into behavioral data.... We are the sources of surveillance capitalism’s crucial surplus: the objects of a technologically advanced and increasingly inescapable raw-material-extraction operation ... Surveillance capitalist firms, beginning with Google, dominate the accumulation and processing of information, especially information about human behavior. They know a great deal about us, but our access to their knowledge is sparse: hidden in the shadow text and read only by the new priests, their bosses, and their machines.”³⁴

57. Google offers services to users (such as Search, Gmail, Chrome, Maps, Meet, Calendar, Drive, and YouTube) that are both convenient and powerful, and their power can be unlocked by the simple click of a button indicating that a user consents to Google’s privacy policy and terms of service. The tradeoff for the use of those services is surveillance. (Zuboff notes that “‘privacy’ policies are more aptly referred to as surveillance policies.”³⁵)

58. Google also offers free software development kits (SDKs) to app developers (such as the Firebase SDK and Google Mobile Ads SDK) that developers can use to build and monetize their apps. Google uses these services to surveil users on non-Google apps, without making clear to developers that there is no Google control that would allow users to escape this surveillance.

59. To defeat the perception that its services involve an all-or-nothing choice, Google also represents that users can have control and privacy—such as by adjusting the WAA and sWAA controls.

60. However, many documents produced by Google demonstrate that the actual functioning of the WAA and sWAA controls has been unclear to many Google employees. For example, in a 2019 internal document on trust and privacy, user experience (UX) researcher David Akers noted that “Google’s own systems have become more complex over time, making it much harder for people to make decisions related to privacy. A control like ‘WAA’ was once relatively simple, but with the proliferation of personalization has now become a coarse-grained control that affects many products. The reality is so complex with WAA that not even *we* understand exactly what happens. (There are no universally accepted policies for how Google products should respond to the WAA setting.)”³⁶ The authors went on to state that by meeting the company’s promise to “make it simple” (as Google CEO Sundar Pichai stated in a *New York Times* op-ed³⁷), one goal is

³⁴ Shoshana Zuboff, *The Age of Surveillance Capitalism*, Public Affairs, <https://archive.org/details/shoshanazubofftheageofsurveillancecapitalism> (2019), pp. 14, 17, 186.

³⁵ Shoshana Zuboff, *The Age of Surveillance Capitalism*, Public Affairs, <https://archive.org/details/shoshanazubofftheageofsurveillancecapitalism> (2019), p. 238.

³⁶ GOOG-RDGZ-00025811 at -12.

³⁷ Sundar Pichai, “Google’s Sundar Pichai: Privacy should not be a luxury good,” *New York Times*, <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html> (May 7, 2019).

Rodriguez v. Google

to encourage users to feel “warm/fuzzy about Google,” and confident that the company “has people’s best interests at heart.”³⁸

61. While the promise of privacy control is important in allowing Google to attract and retain users, that promise does not necessarily translate into actually providing privacy. Given that Google benefits by increasing the scope of its collection and storage of user data, it has strong incentives to overstate the effectiveness of the promised privacy control mechanisms of its numerous services. Google is able to increase its profits from its actual customers—that is, advertisers—by reducing the privacy of its intended audience—that is, users. Google is a more profitable company if users access the Internet using Google’s Chrome browser, check their messages in Gmail, use Google Search, watch videos on YouTube, or obtain directions from Google Maps, and use websites and apps that use Google services like Analytics—either on a personal computer or a phone—without thinking about how much personal information they’re revealing to Google when they do all of those things.

62. As discussed below, this is why it is so important for privacy controls like WAA and sWAA to actually deliver privacy. When average citizens wake up in the morning, they don’t consider that they’re going to allow a bunch of unknown corporations to track them throughout the day; they just put their mobile phone in their pocket and go about their business. It’s different when people use these privacy controls. When users choose to set their WAA or sWAA controls to “off,” they are affirmatively expressing their choice of long-term privacy.

63. Google executives have belittled such concerns, even though Google has, more than any other company on the planet, established surveillance as a phenomenally profitable business model. In a 2009 interview, then-CEO Eric Schmidt said, “If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”³⁹

64. Schmidt’s 2009 statement is not the only time that Google’s leaders have discounted the significance of privacy to their users. In an interview with Charlie Rose at TED2014, Google cofounder Larry Page characterized as overblown public concerns about the privacy of individual medical records and the risk of entrusting even purportedly anonymized records to Google. Page suggested that since he had benefited from sharing his own medical troubles with the world, users of his company’s products should not be concerned by his and his colleagues’ dream of amassing “everyone’s medical records” for the purpose of analyzing them and sharing them with researchers.⁴⁰

65. Consider the following statement, from former Google CEO Eric Schmidt’s 2013 book, *The New Digital Age*:

“We believe that modern technology platforms, such as Google, Facebook, Amazon and Apple, are even more powerful than most people realize..., and what gives them power is their ability to grow—specifically, their speed to scale. Almost nothing, short of a biological

³⁸ GOOG-RDGZ-00025811 at -13.

³⁹ *CNBC*, “Google CEO Eric Schmidt on privacy,” <https://www.youtube.com/watch?v=A6e7wfDHzew> (December 8, 2009).

⁴⁰ Larry Page and Charlie Rose, “Where’s Google going next?” TED, https://www.ted.com/talks/larry_page_where_s_google_going_next?language=en (March 2014).

Rodriguez v. Google

virus, can scale as quickly, efficiently or aggressively as these technology platforms and this makes the people who build, control, and use them powerful too.”⁴¹

2.3. Privacy Has Become More Important with Widespread Corporate Surveillance

66. US citizens have been harmed by the vulnerability of information collected online and stored by numerous companies. Major data leaks abound. These include:

- Yahoo! (2017: 3 billion user accounts hacked),⁴²
- Target (2013: 40 million credit and debit records and 70 million customer records stolen in 2013),⁴³
- Facebook (2021: 533 million users’ phone numbers and other personal data leaked online),⁴⁴
- Marriott Corporation (2018: 383 million booking records, 5.3 million unencrypted passport numbers and tens of millions of encrypted records; 2020: 5.2 million guest records; 2022: 20GB of data, including credit card information and internal company documents),⁴⁵ and
- Experian (2015: 15 million T-Mobile accounts; 2020: 24 million individual accounts and 800,000 business accounts; 2021: 220 million accounts, representing nearly every citizen of Brazil.)⁴⁶

⁴¹ Eric Schmidt and Jared Cohen, *The New Digital Age*, Knopf https://archive.org/details/newdigitalageres0000schm_w0t9 (2013), p. 25.

Knopf Doubleday Publishing Group, “Google executives to publish new book with Knopf,” <http://knopfdoubleday.com/2012/12/03/google-executives-to-publish-new-book-with-knopf> (December 3, 2012).

⁴² Selena Larson, “Every single Yahoo account was hacked—3 billion in all,” *CNN Business*, <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html> (October 4, 2017).

⁴³ Michael Kassner, “Anatomy of the Target data breach,” *ZD Net*, <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned> (February 2, 2015).

⁴⁴ Aaron Holmes, “533 million Facebook users’ phone numbers and personal data have been leaked online,” *Business Insider*, <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4> (April 3, 2021).

⁴⁵ Seena Gressin, “The Marriott data breach,” US Federal Trade Commission, <https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach> (December 4, 2018).

Brandon Vigliarolo, “Marriott Hotels admits to third data breach in 4 years,” *The Register*, https://www.theregister.com/2022/07/06/marriott_hotels_suffer_yet_another (July 6, 2022).

⁴⁶ Jim Finkle, “Massive data breach at Experian exposes personal data for 15 million T-Mobile customers,” *Huffington Post/Reuters*, https://www.huffpost.com/entry/experian-hacked-tmobile_n_560e0d30e4b0af3706e0481e (October 2, 2015).

Phil Muncaster, “Experian data breach hits 24 million customers,” *InfoSecurity Magazine*, <https://infosecurity-magazine.com/news/experian-data-breach-24-million> (August 20, 2020).

Rodriguez v. Google

67. Smaller but equally notorious incidents such as the 2015 Ashley Madison breach (which exposed 32 million users' personal information) that changed the lives of many of its users, and continue to put them at risk.⁴⁷

68. Such incidents provide important context for understanding Google's representations and the expectations of users who turned off their WAA or sWAA settings. Given the frequency with which these huge troves of data have been compromised, including various reported Google data breaches and privacy violations,⁴⁸ it is not surprising that approximately 80% of respondents to a 2021 Ipsos survey expressed great concern about data privacy and security.⁴⁹ Now more than ever, people rightfully seek to use the Internet without being tracked. They use privacy preserving browsers like DuckDuckGo, ad blockers like Privacy Badger and Adblock Plus, and send their messages using the encrypted Signal app. It is within this context that Google offers the WAA and sWAA controls. And whereas features such as Google Chrome's Incognito purport to offer privacy only for the duration of a browsing session, the WAA and sWAA controls purport to offer privacy across a range of apps and services for as long as the controls are set to "off."

69. Public concern about privacy has also escalated during the rise of online tracking for purposes of advertising and "website analytics" and "app analytics"—that is, the systematic collection, reporting and analysis of website and app data for the purpose of understanding site and app usage and maximizing their effectiveness and monetization. This capability has strengthened with Google's introduction of software development kits that developers use to build apps, including Google's Firebase SDK.

3. User Data

3.1. Personal Data Is a Byproduct of Computing

70. Computers and other devices (including phones and tablets) constantly produce data. Data is their input, output, and a byproduct of everything they do. In the normal course of operations, computers and these other devices continuously document their activity. They sense and record more than most users are informed of.

71. Consider a single application: a word processor. Word processors keep a record of everything a user has written into a document, including their drafts and changes. Hit "save," and

Brian Krebs, "Experian API exposed credit scores of most Americans," *Krebs on Security*, <https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans> (April 28, 2021).

Angelica Mari, "Experian challenged over massive data leak in Brazil," *ZD Net*, <https://www.zdnet.com/article/experian-challenged-over-massive-data-leak-in-brazil> (February 20, 2021).

⁴⁷ Zak Doffman, "Ashley Madison hack returns to 'haunt' its victims: 32 million users now watch and wait," *Forbes*, <https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait> (February 1, 2020).

⁴⁸ Michael X. Heiligenstein, "Google data breaches: Full timeline through 2022," *Firewall Times*, <https://firewalltimes.com/google-data-breach-timeline> (January 18, 2022).

⁴⁹ Chris Jackson and Catherine Morris, "Americans report high levels of concern about data privacy and security," *Ipsos*, <https://www.ipsos.com/en-us/americans-report-high-levels-concern-about-data-privacy-and-security> (March 16, 2021).

Rodriguez v. Google

the word processor records the new version, but doesn't erase the earlier ones until the computer needs the disk space for something else. Don't hit "save," and the word processor will automatically save temporary versions at some preset interval. When a document is created, the word processor records who created it; when multiple people edit the document, the word processor keeps a record of everyone who edits it.

72. On the Internet and on mobile devices, the data produced by even a single individual multiplies: records of websites visited, smartphone apps run, ads clicked on, words typed, location information, device information, and other information. An individual user's computer or mobile device, their ISP's servers, and the computers hosting the sites they visit and apps they use all produce data. Individual apps may be generating data about their use: what the individual does, what they look at, what features are enabled and disabled on their devices, and so on. Data may also be sent to or collected by parties unknown to the individual. This data can easily be enough to uniquely identify a person: or at least a single computer, phone, or tablet.⁵⁰

73. Communication with family, friends, co-workers, clients, and casual acquaintances is increasingly mediated by computers and mobile devices by means of email, text messaging, social media sites, and smartphone apps. Data is a by-product of this high-tech socializing. Both data (emails, text messages, voice and video recordings) and metadata (sender, receiver, date and time, size of message, duration of communication, etc.) are collected from these systems. Computerized systems don't just transfer data; they also create records of interpersonal interactions.

74. A technically unsophisticated citizen walking around outside, cell phone in pocket, might not think that they're producing data, but they are. Their phone is constantly calculating its location by touching base with nearby cellular towers.

75. Of course, if our citizen actually uses that phone, they produce metadata: numbers dialed, calls placed and calls received, text messages sent and received, call time and duration, and so on. If the phone is a smartphone, it's also a computer; all of the apps installed on it produce data when they're used—and sometimes even when they're not. Modern smartphones often have a GPS receiver, which produces even more precise location information than cell tower location alone. The GPS receiver is capable of pinpointing its host's location to within 16 to 27 feet; cell towers, by comparison, are accurate to about a 2,000-foot radius of the tower.⁵¹

76. When our citizen purchases something in a store, more data is produced. More often than not, the cash register is a dedicated computer, and it creates a record of all purchases, with their time and date. That data flows into the merchant's computer system. Unless cash payment is made, credit or debit card information is tied to that purchase, enabling the purchaser to be

⁵⁰ Peter Eckersley, "How unique is your web browser?" *Proceedings of the 10th International Conference on Privacy Enhancing Technologies, Berlin*, <https://coveryourtracks.eff.org/static/browser-uniqueness.pdf> (July 2010).

⁵¹ Paul A. Zandbergen, "Accuracy of iPhone locations: A comparison of assisted GPS, WiFi and cellular positioning," *Transactions in GIS* 13, https://www.paulzandbergen.com/PUBLICATIONS_files/Zandbergen_TGIS_2009.pdf (June 26, 2009).

Paul A. Zandbergen and Sean J. Barbeau, "Positional accuracy of assisted GPS data from high-sensitivity GPS-enabled mobile phones," *Journal of Navigation* 64, http://www.paulzandbergen.com/files/Zandbergen_Barbeau_JON_2011.pdf (July 2011).

Rodriguez v. Google

individually identified. That data is also sent to the credit card company, and is incorporated into the purchaser's monthly bill. If the purchaser uses a customer loyalty account, their identity and purchases will also be recorded, even if they paid in cash. There may be a video camera in the store, installed to record evidence in case of theft or fraud. Cameras are also installed near many automatic teller machines. There are more cameras outside, monitoring buildings, sidewalks, roadways, and other public spaces.

77. Snap a photo, and still more data is created. Date, time, and location of the photo's capture; information about the camera, lens, and settings; and an ID number of the camera itself are all embedded in the photo file. If that photo is uploaded to a cloud storage provider or social media site, its metadata often remains attached to the file.⁵²

78. It wasn't always like this. In the era of newspapers, radio, and television, citizens received information, but no record of the consumption was created. Now, news and entertainment are conveyed online. Face-to-face and hardwired telephone communication used to be the norm; conversations now take place via email, cell phones, direct messaging, and apps such as Facebook Messenger and WhatsApp. Shoppers who used to make their purchases in cash at brick-and-mortar stores now use credit cards online and payment services such as PayPal, Venmo and Zelle. Travelers used to pay their bus and subway fares, road tolls, and parking fees with coins at a tollbooth, turnstile, or parking meter; now, fare cards, E-ZPass, and pay-and-display systems—usually connected to an individual's credit card and always to their license plate—are now de rigueur. (Increasingly, governments are removing the option of paying for transit fees in cash.⁵³) Taxis used to accept cash only; credit cards now make passengers easier to track—and easier to reunite with their lost possessions. Smartphones enable access to networked taxi systems like Uber and Lyft, which produce data records of the transaction, plus pickup and drop-off locations. With a few exceptions, computers are now ubiquitous in commerce and in a great deal of social life.

79. Computers that connect to the Internet are embedded into increasing numbers of consumer products. Nest, which Google purchased in 2014 for more than \$3 billion, manufactures an Internet-enabled thermostat that adapts to users' behavior patterns and responds to activity on the power grid. But to do all that, it records more than a home's energy usage: it also tracks and

⁵² Benjamin Henne, Maximilian Koch, and Matthew Smith, "On the awareness, control and privacy of shared photo metadata," Distributed Computing & Security Group, Leibniz University, presented at the Eighteenth International Conference for Financial Cryptography and Data Security, Barbados, http://ifca.ai/fc14/papers/fc14_submission_117.pdf (March 3-7, 2014).

Thomas Germain, "How a photo's hidden 'Exif' data exposes your personal information," *Consumer Reports*, <https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data-a2386546443> (December 6, 2019).

⁵³ Christian M. Wade, "Cashless tolls on Mass. Pike raise revenue, privacy concerns," *Salem News*, https://www.salemnews.com/news/state_news/cashless-tolls-on-mass-pike-raise-revenue-privacy-concerns/article_325861fa-079c-5a82-b155-0a7339e2af6e.html (September 22, 2016).

Frank Esposito, "Cashless tolls: Welcome to the dark future," *Rockland/Westchester Journal News*, <https://www.lohud.com/story/news/investigations/2018/04/11/cashless-tolls-dark-future/439131002> (April 11, 2018).

Rodriguez v. Google

records its temperature, humidity, ambient light, and any movement near the thermostat.⁵⁴ A smart refrigerator has been developed that tracks the expiration dates of food, and a smart air conditioner can learn users' preferences and maximize energy efficiency.⁵⁵ Nest also produces a smart smoke and carbon monoxide detector and is planning a whole line of additional home sensors.⁵⁶ Many other companies are working on a variety of smart appliances, widespread adoption of which will facilitate the smart power grid, which promises to reduce energy use and greenhouse gas emissions.⁵⁷

80. Modern cars are loaded with computers that record speed, pressure on the pedals, steering wheel position, and more.⁵⁸ Much of this data is automatically recorded in a black box recorder, which facilitates reconstruction of traffic accidents, and can also be deployed to monitor the use of rental and fleet vehicles. Sensors in each tire gather pressure data, and enable drivers to avoid a surprise flat. When a car is brought to a mechanic for repairs, the first thing the mechanic will do is access all that data to diagnose any problems. Modern connected cars generate up to 25 gigabytes of data per hour;⁵⁹ one fully autonomous car could produce between 380 terabytes to 5,100 terabytes of data in a single year.⁶⁰

81. In 2010, Google CEO Eric Schmidt stated that "From the dawn of civilization to 2003, five exabytes of data were created. The same amount was created in the last two days."⁶¹ While

⁵⁴ Nest, "Nest Learning Thermostat," <https://files.bbystatic.com/vhTV4lnOCsNyVEpOkxhbpQ%3D%3D/0541791a-0142-49e2-a7ca-2bf505340b4d.pdf> (2018).

⁵⁵ Eliza Barclay, "The 'smart fridge' finds the lost lettuce, for a price," *The Salt: What's On Your Plate*, National Public Radio, <https://www.npr.org/sections/thesalt/2012/05/03/151968878/the-smart-fridge-finds-the-lost-lettuce-for-a-price> (May 4, 2012).

Ry Crist, "Haier's new air conditioner is the first Apple-certified home appliance," *CNET*, <https://www.cnet.com/home/kitchen-and-household/haiers-new-air-conditioner-is-the-first-apple-certified-home-appliance> (January 8, 2014).

⁵⁶ Nest, "Nest Protect (Wired 120V ~ 60Hz) user's guide," [https://nest.com/support/images/misc-assets/Nest-Protect-\(Wired-120V\)-User-s-Guide.pdf](https://nest.com/support/images/misc-assets/Nest-Protect-(Wired-120V)-User-s-Guide.pdf) (June 17, 2014).

⁵⁷ US Department of Energy, "The smart grid: An introduction," [http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages\(1\).pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf) (2008).

⁵⁸ Ben Wojdyla, "How it works: The computer inside your car," *Popular Mechanics*, <http://www.popularmechanics.com/cars/how-to/repair/how-it-works-the-computer-inside-your-car> (February 21, 2012).

Geoffrey A. Fowler, "What does your car know about you? We hacked a Chevy to find out," *Washington Post*, <https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out> (December 17, 2019).

⁵⁹ McKinsey & Company, "What's driving the connected car," <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car> (September 1, 2014).

Hitachi Data Systems, "The internet on wheels and Hitachi, Ltd.," <https://docplayer.net/2138869-The-internet-on-wheels-and-hitachi-ltd-by-hitachi-data-systems.html> (November 2014).

⁶⁰ Simon Wright, "Autonomous cars generate more than 300 TB of data per year," Tuxera, <https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year> (July 2, 2021).

⁶¹ Benjamin Carlson, "Quote of the day: Google CEO compares data across millennia," *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/07/quote-of-the-day-google-ceo-compares-data-across-millennia/344989> (July 3, 2010).

Rodriguez v. Google

there has been some debate regarding the accuracy of Schmidt's estimates,⁶² the impact on society of the dramatic increase in data, and its potential to enable nearly universal surveillance, is significant.

82. This smog of data that society produces is not necessarily a result of malice or deviousness on anyone's part; problems arise, however, when that data is collected, saved or used under false pretenses, such as when users are persuaded to employ settings that falsely claim to offer privacy in general and, even more specifically, respite from collection, saving, or use of information about their online activities. In and of itself, most digital data is simply a natural by-product of computing. This is just the way technology works right now. Data is the exhaust of the information age.

83. Data is not only the exhaust of the information age, it has become the pollution problem of the information age; and protecting privacy is the environmental challenge. How society deals with this challenge—how to ethically collect, store, and dispose of data, and how to call to account those who misuse it—is central to the health of the information economy, and the well-being of the private citizens who contribute data to that economy. Growing awareness of the amount of data produced by users and collected by companies such as Google explains why users seek refuge in the promise and expectation of “privacy control.”

3.2. User Data Encompasses Many Things, Including Data Generated by User Activities

84. User data encompasses a range of information. Certain forms of personally identifying information—for example, name, address, Social Security number, passport or driver's license number, banking and credit card information—are often collected from users of products and services in the course of establishing accounts.

85. The California Consumer Privacy Act defines “personal information” as “information that identifies, relates to, or could reasonably be linked with you or your household. For example, it could include your name, social security number, email address, records of products purchased, Internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.”⁶³

86. That definition is consistent with my understanding as a technologist and with common usage in the field of privacy and security, focusing not only on how information is used but how information could be used (e.g., “can be used”, “could reasonably be linked”).

87. Personally identifiable information is also generated in the course of using customer accounts. These include highly personal records of users' activities online and on mobile devices. Web browsing and app usage result in the accumulation of cookies and the creation of logs containing information from that activity, at ISPs, web hosts and mobile cloud providers. Full URLs often incorporate page titles, and therefore do more than just represent a web address; they may also indicate the content of the page. Smartphone apps often require users to register,

⁶² Bruce Upbin, “The web is much bigger (and smaller) than you think,” *Forbes*, <https://www.forbes.com/sites/ciocentral/2012/04/24/the-web-is-much-bigger-and-smaller-than-you-think> (April 24, 2012).

⁶³ Office of the Attorney General, “California Consumer Privacy Act,” <https://oag.ca.gov/privacy/ccpa> (accessed February 20, 2023).

Rodriguez v. Google

which usually involves providing personal information such as name and email address, in order to unlock their full range of features. Those that require payment will often save users' credit card information. Using mobile devices to access apps can generate device-level information, such as device ID and location, of both registered and unregistered users.

88. As another example of personal content, user interaction with a device results in mouse and cursor movement; analysis of mouse movements is the subject of a Google patent, and is used by many sites for purposes of customer identification.⁶⁴ Shoshana Zuboff has noted that “in addition to key words, each Google search query produces a wake of collateral data such as the number and pattern of search terms, how a query is phrased, spelling, punctuation, dwell times, click patterns, and location.”⁶⁵ Smartphones transmit accelerometer data, which can be used to detect location and speech and keyboard input.⁶⁶ Google was among the first enterprises to recognize that this collateral data generated by its users could be used to improve its search engine, as well as to generate user profiles and advertising products.

3.3. Information from App Activity Is Highly Personal

89. Information about a person's activity while using mobile apps can be highly personal. It may reflect, for example, their political and religious beliefs, their sexual orientation and proclivities, their reproductive cycle and intentions, their medical history and diagnoses, their weight and dietary preferences, their plans to find new employment or move to another location, their experience of domestic abuse, or other aspects of their personal circumstances. And users who have turned their WAA or sWAA controls off have specifically signaled an expectation that their app activity data and the associated content not to be collected and saved by Google.

90. Among the first apps that mobile device users are likely to use are web browser apps. A user's search history can go back many years, in many cases encompassing much of their childhood and adolescence. The proliferation of apps for mobile devices has increased both the variety and granularity of data that can be collected about users. Like websites, apps often place cookies on users' systems; unlike websites, apps often seek to extract data from the phone itself, requesting access to the user's contact list, location, and other information unnecessary for the app's functioning, but valuable for marketing and other purposes.

91. A 2021 study by VPN provider Surfshark found that Meta Platforms apps Facebook, Instagram and Messenger each collected all 32 categories of personal data enumerated by the

⁶⁴ Chris Crum, “Google eyes mouse movement as possible search relevancy signal,” *WebProNews*, <https://www.webpronews.com/google-eyes-mouse-movement-as-possible-search-relevancy-signal> (July 13, 2010).

Antonio Villas-Boas, “Passwords are incredibly insecure, so websites and apps are quietly tracking your mouse movements and smartphone swipes without you knowing to make sure it's really you,” *Business Insider*, <https://www.businessinsider.com/websites-apps-track-mouse-movements-screen-swipes-security-behavioral-biometrics-2019-7> (July 19, 2019).

⁶⁵ Shoshana Zuboff, *The Age of Surveillance Capitalism*, New York: Public Affairs, <https://archive.org/details/shoshanazubofftheageofsurveillancecapitalism> (2019).

⁶⁶ S. Abhishek Anand, et al., “Motion sensor-based privacy attack on smartphones,” arXiv:1907.05972, arXiv.org, <https://arxiv.org/pdf/1907.05972.pdf> (October 19, 2020).

Jingyu Hua, Zhenyu Shen and Sheng Zhong, “We can track you if you take the metro: Tracking metro riders using accelerometers on smartphones,” arXiv:1505.05958, arXiv.org, <https://arxiv.org/abs/1505.05958v1> (May 22, 2015).

Rodriguez v. Google

Apple App Store. Google's YouTube and Chrome apps collected 24 and 13 categories, respectively. Other popular, data-hungry apps include PayPal, Amazon, DoorDash, TikTok, eBay, and Snapchat.⁶⁷ Another analysis of the world's most-used mobile apps found that 60% gathered data resulting from users' private conversations, and that 80% gathered data from their users' message and email traffic.⁶⁸

92. A Stanford University experiment examined the phone metadata of about 500 volunteers over several months. The personal nature of what the researchers could infer from the metadata surprised even them:

- Participant A communicated with multiple local neurology groups, a specialty pharmacy, a rare-condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis.
- Participant B spoke at length with cardiologists at a major medical center, talked briefly with a medical laboratory, received calls from a pharmacy, and placed short calls to a home reporting hotline for a medical device used to monitor cardiac arrhythmias.
- Participant C made a number of calls to a firearms store that specializes in the AR semiautomatic rifle platform, and also spoke at length with customer service for a firearm manufacturer that produces an AR line.
- In a span of three weeks, Participant D contacted a home improvement store, locksmiths, a hydroponics dealer, and a head shop.
- Participant E had a long early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after.

That's a multiple sclerosis sufferer, a heart attack victim, a semiautomatic weapon owner, a home marijuana grower, and someone who had an abortion, all identified from a single stream of metadata generated through their phone calls.⁶⁹ Note that this experiment used cell phone metadata, but the principle demonstrated is also applicable to mobile app data.

93. In a September 2010 interview, Google's CEO Eric Schmidt unapologetically stated that "With your permission you give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about."⁷⁰

94. Many enterprises manipulate what you see according to your user profile: Google Search, Yahoo News, online newspapers like the *New York Times*. This manipulation can be very

⁶⁷ Surfshark, "Uncovering the apps that actually respect your privacy," <https://surfshark.com/apps-that-track-you> (May 14, 2021).

⁶⁸ Tech Shielder, "Hacker hotspots: The apps most vulnerable to cybercrime," <https://techshielder.com/hacker-hotspots-most-vulnerable-apps> (September 2, 2022).

⁶⁹ Jonathan Mayer, Patrick Mutchler and John C. Mitchell, "Evaluating the privacy properties of telephone metadata," *Proceedings of the National Academy of Sciences* 113, no. 20, <http://www.pnas.org/cgi/doi/10.1073/pnas.1508081113> (May 17, 2016).

⁷⁰ Derek Thompson, "Google's CEO: 'The laws are written by lobbyists'," *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/#video> (October 1, 2010).

Rodriguez v. Google

profitable. The first listing in a Google Search result gets 28.5% of the clickthroughs; search results on subsequent pages yield far less engagement.⁷¹ The consequence is that what Internet users see is increasingly tailored to their inferred interests. This leads to a phenomenon that political activist Eli Pariser has called the “filter bubble”: an Internet optimized to individual preferences, where one never need encounter an opinion one doesn’t agree with.⁷²

95. In 2018, the privacy-focused search engine DuckDuckGo conducted a study of the Google Search’s “filter bubble” problem, whereby search results are prioritized according to personal information that Google has collected about individual users, thereby reducing the diversity of information and viewpoints displayed to them. The researchers found that in spite of Google’s claim to have taken steps to reduce the “filter bubble” effect, most searches by study participants using the Chrome browser yielded results that were unique to them.⁷³

3.4. Information about Online Activity Is Unique for Each User

96. American citizens are justified in taking measures to minimize access to their browsing information, since it can be used to identify them. A 2013 study of 368,284 users of both desktop and mobile devices detected a unique browsing history for 69% of participants, and found that out of users for whom at least four visited websites were detected, 97% could be uniquely identified by their browsing history.⁷⁴ There is no reason to expect that the results of this study would be materially different if limited to activity on mobile apps.

97. This browsing information is a rich target for those online businesses that deploy CSS-based detection techniques to collect it. (CSS is an initialism for cascading style sheets, which are used to format web pages and mobile app screens developed with HTML.) An attacker can ascertain URLs visited by a target’s browser through applying CSS styles that differentiate visited and unvisited links. A study of results obtained from over a quarter-million web users found that over 94% of Google Chrome users were vulnerable to CSS-based browser history detection by sites they visited; a test of popular websites detected an average of 62.6% visited locations per client.⁷⁵

98. A 2015 research paper illustrated how third-party cookies can be used by eavesdroppers—these are people who are not the owners of the websites visited, apps used or cookies—to track people on the Internet. Simulating users browsing the web, the authors found that “the adversary

⁷¹ Johannes Beus, “Why (almost) everything you knew about Google CTR is no longer valid,” *Sistrix Blog*, <https://www.sistrix.com/blog/why-almost-everything-you-knew-about-google-ctr-is-no-longer-valid> (July 14, 2020).

⁷² Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin (2011).

⁷³ DuckDuckGo, “Measuring the ‘filter bubble’: How Google is influencing what you click,” *SpreadPrivacy: The Official DuckDuckGo Blog*, <https://spreadprivacy.com/google-filter-bubble-study> (December 4, 2018).

⁷⁴ Lukasz Olejnik, Claude Castelluccia and Artur Janc, “Why Johnny can’t browse in peace: On the uniqueness of web browsing history patterns,” *Annals of Telecommunications* 1-2, <https://hal.inria.fr/file/index/docid/747841/filename/johnny2hotpet-finalcam.pdf> (June 2013).

⁷⁵ Artur Janc and Lukasz Olejnik, “Web browser history detection as a real-world privacy threat,” *ESORICS’10: Proceedings of the 15th European Conference on Research in Computer Security*, <http://cds.cern.ch/record/1293097/files/LHCb-PROC-2010-036.pdf> (September 20, 2010).

Rodriguez v. Google

can reconstruct 62–73% of a typical user’s browsing history.”⁷⁶ Advertising identifiers (e.g., AdID, IDFA), like cookies, identify a device, and can therefore be used for similar purposes. There is no reason to believe that the results of this study would differ if limited to such advertising identifiers and activity on mobile apps.

99. Each smartphone owner installs a unique constellation of apps on their phones, and uses a subset of them. A recent survey of over 3,700 mobile phone users found that the average participant had 40 apps installed on their phone, and spent 89% of their time on 18 of those apps. Respondents in the 21–30-year-old age range typically had more than 67 apps installed on their phone, and commonly used 25 of them.⁷⁷

3.5. Online Advertising Has Risks for Users

100. The rise in online advertising (including advertisements delivered through apps on mobile devices) has enabled an increase in the ability of hostile nations to influence American citizens. In 2017, following Facebook’s acknowledgement that it had sold thousands of political ads to a Russian government agency seeking to influence the 2016 presidential election,⁷⁸ Google disclosed that during the leadup to the election, accounts linked to Russia had purchased an unknown number of ads costing less than \$100,000 for display on the company’s platforms, including via the YouTube and Gmail websites and apps, and through the DoubleClick ad network.⁷⁹ However, in a *Washington Post* op-ed, media strategist Jason Kint observed that it would be impossible to determine how many political ads by foreign actors had actually been displayed via Google during the 2016 election season, thanks to Google’s successful lobbying for ads on its platform to be exempt from disclosures generally required of campaigns.⁸⁰

101. The online advertising ecosystem can also be exploited on a small scale, to surveil both individuals and communities. For example, in 2017, researchers at the University of Washington found that third parties with access to a phone’s unique ID could track users’ location and mobile app usage by targeting that ID with low-cost, location-based ads. The authors noted that such advertising-based intelligence could be used by ideological vigilantes, stalkers, burglars, and

⁷⁶ Steven Englehardt, et al., “Cookies that give you away: The surveillance implications of web tracking,” *WWW ‘15: Proceedings of the 24th International Conference on World Wide Web*, https://senglehardt.com/papers/www15_cookie_surveil.pdf (May 18, 2015).

⁷⁷ Maitrik Kataria, “App usage statistics 2022 that’ll surprise you (updated),” *Simform*, <https://www.simform.com/blog/the-state-of-mobile-app-usage> (January 5, 2021; last updated November 11, 2022).

⁷⁸ Graham Kates, “Facebook, for the first time, acknowledges election manipulation,” CBS News, <https://www.cbsnews.com/news/facebook-for-the-first-time-acknowledges-election-manipulation> (April 28, 2017).

⁷⁹ Elizabeth Dwoskin, Adam Entous and Craig Timberg, “Google uncovers Russian-bought ads on YouTube, Gmail and other platforms,” *Washington Post*, <https://www.washingtonpost.com/news/the-switch/wp/2017/10/09/google-uncovers-russian-bought-ads-on-youtube-gmail-and-other-platforms> (October 9, 2017).

⁸⁰ Jason Kint, “The Russia ad story isn’t just about Facebook. It’s about Google, too,” *Washington Post*, https://www.washingtonpost.com/opinions/the-russia-ad-story-isnt-just-about-facebook-its-about-google-too/2017/10/31/061055da-be5d-11e7-8444-a0d4f04b89eb_story.html (October 31, 2017).

Rodriguez v. Google

blackmailers, to identify Grindr users, Quran reciters, ex-lovers, purchasers of luxury goods, and brothel patrons.⁸¹

102. Internet advertising is an enormous drain on computing resources whether it occurs on a website or a mobile platform. A 2018 study estimated that 11.53–159.93 million tons of carbon dioxide were emitted to produce the electricity consumed by online advertising, nearly one-fifth of which was associated with invalid traffic.⁸² A 2020 study comparing page load time of computers running ad blockers to those without them found that page load time dropped between 11% and 28.5% for computers with ad blockers. It was estimated that users could save more than 100 hours of page load time per year with the best-performing blocker, and forecast considerable savings in money and energy if all Internet users were to adopt ad-blocking technology on their devices.⁸³ Additionally, a 2022 study of French media websites found that “between 32% and 70% of the energy consumed by the browser and network is due to monetization,” and that “on average, using an ad blocker reduces emissions by 37%.”⁸⁴

3.6. User Activity on Mobile Apps Is Sensitive Information

103. Once, web browsers were primary means by which users accessed the Internet, and there were only a few of them: Mosaic, Netscape Navigator, Internet Explorer, Opera, Firefox, and maybe a few more. Today, users of mobile devices can access the Internet through literally millions of different apps.

104. This increasing app usage has many unique privacy implications. One involves the possibility of circumvention by the apps themselves. A 2019 study of over 88,000 Android apps found that hundreds circumvented the Android permissions system to collect user information. This circumvention occurred through side channels, which exploit unintended features of the permissions system, and covert channels, which involve the collusion of two apps. For example, the researchers found that the Shutterfly app, with millions of downloads, sent users’ precise geolocation data to its servers, in the absence of a location permission, by parsing the EXIF data from users’ photos.⁸⁵

105. Data collected from users’ app activity (and then saved by either the app developers or third parties like Google) can have real-world consequences given changing federal and state laws. The US Supreme Court’s recent decision to overturn *Roe v. Wade* and concurrent efforts in

⁸¹ Paul Vines, Franziska Roesner and Tadayoshi Kohno, “Exploring ADINT: Using ad targeting for surveillance on a budget, or How Alice can buy ads to track Bob,” ACM Workshop on Privacy in the Electronic Society, WPES ’17, Dallas, Texas, <https://dl.acm.org/doi/pdf/10.1145/3139550.3139567> (October 30, 2017).

⁸² Matti Pärssinen, et al., “Environmental impact assessment of online advertising,” *Environmental Impact Assessment Review* 73, <https://www.sciencedirect.com/science/article/pii/S0195925517303505#!> (November 2018).

⁸³ Joshua M. Pearce, “Energy conservation with open source ad blockers,” *Technologies* 8, no. 18, <https://www.mdpi.com/2227-7080/8/2/18/htm> (March 30, 2020).

⁸⁴ Caroline Schneider and Clément Le Biez, “Media websites: 70% of the carbon footprint caused by ads and stats,” Marmelab, <https://marmelab.com/blog/2022/01/17/media-websites-carbon-emissions.html> (January 17, 2022).

⁸⁵ Joel Reardon, et al., “50 ways to leak your data: An exploration of apps’ circumvention of the Android permissions system,” PrivacyCon 2019, Washington, D.C., https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serje_egelman.pdf (June 27, 2019).

Rodriguez v. Google

numerous states to criminalize abortion have precipitated concern about the extent to which data from menstruation-tracking apps could be used as evidence against women who obtain abortions. These apps can reveal not only details of the menstrual cycle, but also the lack of menstruation (which often suggests pregnancy) and its resumption following birth, stillbirth or abortion. The data gathering process for health apps is not governed by HIPAA, the federal law that covers information shared with doctors and other health care providers.⁸⁶ Given that browser history has been used as evidence in prosecutions of women who have sought to terminate a pregnancy,⁸⁷ concern about the inappropriate use of data pertaining to one's reproductive function is reasonable.

106. This concern is not just speculative. In January 2021, the FTC announced a complaint against the developer of the Flo Period & Ovulation Tracker, alleging that “Flo disclosed health data from millions of users of its Flo Period & Ovulation Tracker app to third parties that provided marketing and analytics services to the app, including Facebook’s analytics division, Google’s analytics division, Google’s Fabric service, AppsFlyer, and Flurry.”⁸⁸ A Consumer Reports study of period tracker apps found that at least one app, Lady Cycle, incorporated a tracker from the Firebase SDK.⁸⁹ The nominally-encrypted period-tracking app Stardust was found to be sharing user phone numbers with a third-party analytics firm.⁹⁰

107. The UK-based Organization for the Review of Care and Health Apps recently analyzed the data permissions and use of 25 menstrual tracking apps and found that 21 shared data with third parties, 70% of those for marketing purposes, including sale of users’ contact information. Nearly half of the apps failed to meet minimum requirements for data security, and apps providing the most sophisticated fertility monitoring were among those with the worst data security scores.⁹¹ A 2019 Gallup survey concluded that one in five adults in the US—and nearly

⁸⁶ Alisha Haridasani Gupta and Natasha Singer, “Your app knows you got your period. Guess who it told?” *New York Times*, <https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html> (January 28, 2021).

⁸⁷ Cat Zakrzewski, Pranshu Verma and Claire Parker, “Texts, web searches about abortion have been used to prosecute women,” *Washington Post*, <https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/> (July 3, 2022).

⁸⁸ US Federal Trade Commission, “Developer of popular women’s fertility-tracking app settles FTC allegations that it misled consumers about the disclosure of their health data,” <https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about> (January 13, 2021).

⁸⁹ Catherine Roberts, “Period tracker apps and privacy,” *Consumer Reports*, <https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145> (May 25, 2022).

⁹⁰ Sarah Perez and Zack Whittaker, “Period tracker Stardust surges following Roe reversal, but its privacy claims aren’t airtight,” *Tech Crunch*, <https://techcrunch.com/2022/06/27/stardust-period-tracker-phone-number/> (June 27, 2022).

⁹¹ ORCHA, “Data privacy matters...Period: Data security of period tracking apps,” Organization for the Review of Care and Health Apps, <https://info.orchahhealth.com/data-security-period-tracking-apps> (August 9, 2022).

Rosie Taylor, “Popular period-tracking apps are sharing sensitive personal data with advertisers including cycle dates, contraception use and how often you’re having sex, study reveals,” *Daily Mail*, <https://www.dailymail.co.uk/sciencetech/article-11045653/Popular-period-tracking-apps-sharing-sensitive-personal-data-advertisers-study-finds.html> (July 25, 2022).

Rodriguez v. Google

half of women under 50—used health apps or wearable trackers.⁹² The data generated by all of these apps is very personal information.

108. App data may be collected and saved not only by the app developer but also by third parties, including Google. This can be accomplished by means of software development kits (SDKs). SDKs consist of pre-coded libraries of functions that can be readily incorporated into their apps, and offer significant convenience to developers. However, that convenience can come at a cost, especially when developers are careless about user security. In 2018, a security researcher from Kaspersky Labs demonstrated that millions of apps that incorporated third-party software libraries were transmitting unencrypted personal user data—including names, ages, incomes, phone numbers, email addresses, birthdates, usernames, and GPS coordinates—to advertisers’ servers using the unencrypted HTTP protocol rather than encrypted HTTPS.⁹³

109. A *New York Times* investigation of SDK usage found that one app—the aptly-named Period Tracker—contained 26 different SDKs, including ones from Facebook and Google. The hookup-facilitating Feeld app had 42 different SDKs in its Android version and 52 in its iOS version. Of SDKs, one advertising executive stated, “every app is potentially leaking data to five or ten other apps. Every SDK is taking your data and doing something different—combining it with other data to learn more about you. It’s happening even if the company says we don’t share data. Because they’re not technically sharing it; the SDK is just pulling it out. Nobody has any privacy.”⁹⁴

110. Google collects data relating to user activity on numerous apps. If Google collects data that identifies a user from any one of those apps (e.g., a unique browsing history, username, email address, or name), then all data that Google collects about that user, on any device, becomes identifiable.

4. The Value of User Data

4.1. User Data Generates Billions in Corporate Revenue

111. The largest online companies are highly incentivized to capitalize on their users’ data to generate billions in revenue. Together, Google and Facebook dominate this field: in 2022,

⁹² Justin McCarthy, “One in five U.S. adults use health apps, wearable trackers,” Gallup, <https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx> (December 11, 2019).

⁹³ Roman Unuchek, “Leaking ads: Is user data truly secure?” RSA 2018, San Francisco, <https://published-prd.lanyonevents.com/published/rsaus18/sessionsFiles/8161/ASEC-T08-Leaking-Ads-Is-User-Data-Truly-Secure.pdf> (April 16-20, 2018).

⁹⁴ Charlie Warzel, “The loophole that turns your apps into spies,” *New York Times*, <https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html> (September 24, 2019).

Rodriguez v. Google

Google took in \$224.473 billion in digital advertising revenue,⁹⁵ and Facebook \$113.642 billion.⁹⁶ These revenues are tied to data-driven advertising.

112. Here's an example of the value of personal data. Dataium was a company (acquired in 2015 and retired three years later)⁹⁷ that tracked people as they shopped for cars online. It monitored their visits to different manufacturers' websites: what types of cars they were looking at, what options they clicked on for more information, what sorts of financing options they researched, how long they lingered on any given page. Dealers paid for this information—not just information about the cars they sold, but the cars people looked at that were sold by other manufacturers. They paid for this information so that when potential buyers walked into a showroom, they could more profitably sell them a car.⁹⁸

113. For a ballpark estimate, that information might have cost the customer \$300 extra on the final price of the car; that is, it was worth no more than \$300 for each customer to protect themselves from Dataium's data-scraping. But with 16 million cars sold annually in the US, even if one assumes that Dataium had customer information relevant to just 2% of them, it was worth \$100 million to the company to ensure that its tactics worked.

114. This asymmetry is why market solutions tend to fail. It's a collective action problem. Even though it might have been worth \$100 million to society to protect citizens from Dataium, those citizens couldn't necessarily coordinate effectively. Dataium effectively banded the car dealers together, but there was no analogous process whereby customers could band together.

115. Problems arise not only in terms of collection but also when that information is being used in ways we didn't intend: when it is saved, shared, sold, correlated, and exploited to manipulate people. Restrictions on how data can be saved and used are important, especially restrictions on uses that differ from the purposes for which data was collected.

116. Other problems arise when corporations treat their underlying algorithms as trade secrets: Google's search algorithms (such as PageRank, which determines what search results you see and in what order), and credit-scoring systems, are two examples. The companies that use

⁹⁵ Alphabet, Inc., "Form 10-K," United States Securities and Exchange Commission, https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf?cache=5ae4398 (February 3, 2023).

⁹⁶ Meta Platforms, Inc., "Form 10-K," United States Securities and Exchange Commission, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/e574646c-c642-42d9-9229-3892b13aabfb.pdf> (February 3, 2023).

⁹⁷ Geert de Lombaerde, "\$2B company buys local auto shopping data venture," *Nashville Post*, https://www.nashvillepost.com/2b-company-buys-local-auto-shopping-data-venture/article_37f98c02-ed8e-5bba-b069-cb251e8eb11a.html (April 10, 2015).

S&P Global, "S&P Global, now part of S&P Global acquired business asserts of Dataium," <https://spglobal.com/en/enterprise/btp/dataium.html> (accessed February 20, 2023).

⁹⁸ Jennifer Valentino-DeVries and Jeremy Singer-Vine, "They know what you're shopping for," *Wall Street Journal*, <http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214> (December 7, 2012).

Jeremy Singer-Vine, "How Dataium watches you," *Wall Street Journal*, <http://blogs.wsj.com/digits/2012/12/07/howdataium-watches-you> (December 7, 2012).

Rodriguez v. Google

proprietary algorithms have legitimate concerns about trade secrecy. They're worried that competitors will copy them and that people will figure out how to game them. But this secrecy prevents transparency, which is critical when the algorithms in question have a direct impact on the public.⁹⁹ Google collects user data for its own financial benefit, including to refine Google's search and ad bidding algorithms, but there is limited information available in terms of what that means for user privacy.

117. Consumer surveillance is much older than the Internet. Before the Internet, there were four basic surveillance streams. The first flowed from companies keeping records on their own customers. The second stream flowed from direct mail marketing, which involved the creation of lists of people who might welcome a vendor's promotional or fundraising mail so that time, money, materials, and effort would not be spent to solicit those who would be unreceptive. Direct mail lists were sorted according to demographic characteristics; many had their beginnings as aggregated magazine subscription lists, or customer lists from related enterprises.

118. The third surveillance stream came from credit bureaus, which collected detailed information about individuals' financial transactions, and sold that information to banks needing to determine the creditworthiness of potential customers. This detailed, expensive form of data collection was only cost-effective for high-risk matters such as credit card approvals, apartment leases, mortgages, and the like.

119. The fourth surveillance stream flowed from government. This stream consisted of public records: birth and death certificates, driver's license records, voter registration records, various permits and licenses, court documents, and so on. Private enterprises have increasingly been able to acquire or purchase this public data for their own use; use cases include people-search websites, websites featuring arrest records, and real estate websites.¹⁰⁰

120. Credit bureaus and direct marketing companies eventually combined these four streams to become modern-day data brokers like Acxiom.¹⁰¹ Data brokers buy citizens' personal data from private businesses, combine it with publicly available information about them, and sell the results. And they've ridden the tides of computerization. The more data an individual produces, the more information about them can be collected and the more accurately they can be profiled,

⁹⁹ Frank Pasquale, "The troubling trend toward trade secret-protected ranking systems," Chicago Intellectual Property Colloquium, Chicago, Illinois, <http://www.chicagoip.com/pasquale.pdf> (April 21, 2009).

¹⁰⁰ Amy Harmon, "As public records go online, some say they're too public," *New York Times*, <https://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html> (August 24, 2001).

Mark Ackerman, "Sales of public data to marketers can mean big \$\$ for governments," CBS Denver, <https://denver.cbslocal.com/2013/08/26/sales-of-public-data-to-marketers-can-mean-big-for-governments> (August 26, 2013).

¹⁰¹ Natasha Singer, "Acxiom, the quiet giant of consumer database marketing: Mapping, and sharing, the consumer genome," *New York Times*, <https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html> (June 16, 2012).

Rodriguez v. Google

leading to still greater revenues for companies that aggregate and market citizens' personal information.¹⁰²

121. The breadth and depth of information that data brokers possess is astonishing.¹⁰³ They collect demographic information: names, addresses, telephone numbers, email addresses, gender, age, marital status, presence and ages of children in household, education level, profession, income level, political affiliation, cars driven, and information about homes and other property. They collect lists of purchases, dates of purchases and forms of payment. They keep track of deaths, divorces, and diseases that run in families. They scrape the web for information about their targets. In 2013, the World Privacy Forum estimated that there were about 4,000 data brokers.¹⁰⁴

122. Data brokers use publicly available and purchased data to sort people into various marketable categories.¹⁰⁵ For example, Acxiom offers lists of "potential inheritors," "adults with senior parent," households with a "diabetic focus" or "senior needs."¹⁰⁶ InfoUSA has sold lists of "suffering seniors" and gullible seniors.¹⁰⁷ In 2011, the data broker Teletrack sold lists of people who had applied for nontraditional credit products like payday loans to companies who wanted to target them for predatory deals.¹⁰⁸ In 2012, Equifax sold lists of people who were late on their mortgage payments to a discount loan company. Because this was financial information, both

¹⁰² Craig Timberg, "Brokers use 'billions' of data points to profile Americans," *Washington Post*, https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html (May 27, 2014).

¹⁰³ *Wall Street Journal*, "What They Know" series index, http://www.wsj.com/public/page/0_0_WZ_0_0448.html.

US Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, "A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes," Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

¹⁰⁴ Pam Dixon, "Testimony of Pam Dixon, Executive Director, World Privacy Forum, before the U.S. Senate Committee on Commerce, Science, and Transportation: What information do data brokers have on consumers, and how do they use it?" World Privacy Forum, <https://www.govinfo.gov/content/pkg/CHRG-113shrg95838/pdf/CHRG-113shrg95838.pdf> (December 18, 2013).

¹⁰⁵ Lois Beckett, "Everything we know about what data brokers know about you," *ProPublica*, <https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you> (September 13, 2013).

¹⁰⁶ Natasha Singer, "Acxiom lets consumers see data it collects," *New York Times*, <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html> (September 5, 2013).

¹⁰⁷ Charles Duhigg, "Bilking the elderly, with a corporate assist," *New York Times*, <http://www.nytimes.com/2007/05/20/business/20tele.html> (May 20, 2007).

¹⁰⁸ US Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, "A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes," Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

Rodriguez v. Google

brokers were fined by the FTC for their actions. However, given the lack of regulation on data collection in other industries, almost everything else is fair game.¹⁰⁹

4.2. Third Parties Perform Electronic Tracking

123. While some businesses seek data about other businesses' customers, the context is very different when a third party is collecting data flows from individual computers, phones, or tablets of the first party's customers. This is akin to installing a classic pen register on a phone, but even more invasive. This practice enables development of extensive and valuable profiles on individuals who have no relationship to those who are seeking information about them.

124. A 2016 analysis of the history of Internet tracking between 1996 and 2016 found that it has become more prevalent, more complex, and more difficult to avoid, and that trackers capture an increasing range of users' online behaviors while using browsers and other mobile apps.¹¹⁰

125. A 2017 study by Exodus Privacy and the Yale University Privacy Lab of trackers incorporated into popular Android phone apps available from the Google Play Store concluded that over 75% of Android apps incorporate at least one third-party tracking plugin. Among these are plugins that enable Google subsidiary Crashlytics to track app crash reports; the service also analyzes app users' behavior.¹¹¹

126. A February 2021 study of web privacy risks arising from the exchange of data between browsers and developers' backend servers found that Google Chrome shared browser information and persistent identifiers that enable long-term tracking, including identification of user location via IP addresses. Chrome assigns persistent identifiers to individual browsers, which are linked to details of visited web pages via the search autocomplete feature.¹¹²

127. The same researchers investigated mobile phone privacy, and found that both iOS and Android devices communicated with Apple and Google, respectively, an average of once every 4.5 minutes, and transmitted telemetry information even when users opted out of this functionality. Although Google cautions that "turning off this feature doesn't affect your device's ability to send the information needed for essential services such as system updates and

¹⁰⁹ US Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, "A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes," Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

¹¹⁰ Adam Lerner, et al., "Internet Jones and the Raiders of the Lost Trackers: An archaeological study of web tracking from 1996 to 2016," 15th USENIX Security Symposium, August 10-12, 2016, Austin, TX, <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner> (2016).

¹¹¹ Sean O'Brien and Michael Kwet, "#BlackFriday announcement from Privacy LAB," Information Society Project, Yale Law School, <https://privacylab.yale.edu/trackers.html> (November 24, 2017).

Alex Hern, "Three quarters of Android apps track users with third party tools—study," *The Guardian*, <https://www.theguardian.com/technology/2017/nov/28/android-apps-third-party-tracker-google-privacy-security-yale-university> (November 28, 2017).

¹¹² Douglas J. Leith, "Web browser privacy: What do browsers say when they phone home?" *IEEE Access* 9, https://www.scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf (March 19, 2021).

Rodriguez v. Google

security,” the study’s authors concluded that the supposedly “essential” data was “extensive, and likely at odds with reasonable user expectations.”¹¹³

5. Limitations on Collecting User Data

5.1. Laws Impose Restrictions on How Companies Can Collect Data

128. The implementation of the European Union’s General Data Protection Regulation (GDPR)¹¹⁴ in 2016 precipitated a conspicuous change in the manner in which websites and mobile apps collected data on their users, or allowed third parties to collect data on their users. Whereas pre-GDPR, websites usually placed cookies on visitors’ browsers without notifying them, and apps gathered various types of data without notifying their users, the new regulation required affirmative notice to and consent by the user before their data can be gathered. Although GDPR is in force in the EU, many US websites and app developers—especially those with many European visitors and customers—have sought to comply with the regulation.

129. In December 2021, the Austrian Data Protection Authority ruled that Google’s flagship web traffic analysis tool Google Analytics cannot be used in accordance with GDPR, since the service creates a unique digital footprint that is transmitted to Google servers in the US, and since the measures implemented to protect this data did not eliminate monitoring and access options by US intelligence services.¹¹⁵

130. The 2018 California Consumer Privacy Act requires both websites and apps to inform users of the sort of information they collect and how it is used, and whether the information is shared and with whom. Users must also be given the right to opt out the collection of data that could be linked to them or their family.¹¹⁶ (Note, again, that I am not an attorney, but am commenting regarding the impact of the GDPR and CCPA on privacy and entities’ responses to this legislation.)

¹¹³ Douglas J. Leith, “Mobile handset privacy: Measuring the data iOS and Android send to Apple and Google,” International Conference on Security and Privacy in Communication Systems (SecureComm) 2021: Security and Privacy in Communication Networks, https://www.scss.tcd.ie/doug.leith/apple_google.pdf (March 25, 2021).

¹¹⁴ European Union, “General data protection regulation (GDPR),” <https://gdpr-info.eu> (April 27, 2016).

¹¹⁵ Datenschutzbehörde, “Information der Datenschutzbehörde zur Entscheidung über die Verwendung von Google Analytics,” Bekanntmachungen der Datenschutzbehörde, <https://www.dsb.gv.at/download-links/bekanntmachungen.html> (December 22, 2021).

Hannah Hewitt, “The Austrian Data Protection Authority ground-breaking Google Analytics decision: Analysis and key takeaways,” Orrick Herrington & Sutcliffe LLP, <https://www.orrick.com/en/Insights/2022/02/The-Austrian-Data-Protection-Authority-Groundbreaking-Google-Analytics-Decision> (February 2, 2022).

¹¹⁶ Joseph J. Lazzarotti and Mary T. Costigan, “CCPA FAQs on cookies,” *National Law Review* 13, no. 52, <https://www.natlawreview.com/article/ccpa-faqs-cookies> (August 29, 2019).

David Zetoony, Christian Auty and Karin Ross, “Answers to the most frequently asked questions concerning cookies and adtech,” Bryan Cave Leighton Paisner, <https://ccpa-info.com/wp-content/uploads/2019/08/Handbook-of-FAQs-Cookies.pdf> (February 2020).

5.2. Restrictions Focus on Collection as Well as Saving and Use

131. Companies that collect user data must focus not only on collection (subject to restrictions on the timing of collection) but also on the appropriate use of data, and its retention and deletion. When storage was expensive, businesses had an incentive to minimize collection, purge useless data, and enforce time limits for data retention in order to minimize the cost of data storage. However, storage is now cheap, thus increasing the risk that companies will retain data far longer than is needed for the successful conduct of business; and the commodification of data translates into business opportunities for those enterprises willing to part with it.

132. Protecting privacy requires regulation in many places: at collection, during storage, upon use, during disputes. The OECD Privacy Framework, adopted in 1980, delineates a set of basic principles of data privacy protection that illustrate the scope of this need:

COLLECTION LIMITATION PRINCIPLE: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

DATA QUALITY PRINCIPLE: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

PURPOSE SPECIFICATION PRINCIPLE: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

USE LIMITATION PRINCIPLE: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.

SECURITY SAFEGUARDS PRINCIPLE: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

OPENNESS PRINCIPLE: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

INDIVIDUAL PARTICIPATION PRINCIPLE: Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to

Rodriguez v. Google

challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

ACCOUNTABILITY PRINCIPLE: A data controller should be accountable for complying with measures which give effect to the principles stated above.¹¹⁷

133. The ACM Code of Ethics and Professional Conduct, which Google, as a leading employer of computer scientists, should be aware of in formulating its course of conduct, speaks to similar effect.

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and **privacy**. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority. [*emphasis added*]

1.3 Be honest and trustworthy.

Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.

1.6 Respect privacy.

The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.

Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the

¹¹⁷ Organization for Economic Cooperation and Development, "The OECD privacy framework," http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (2013).

Rodriguez v. Google

provenance of the data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections.¹¹⁸

134. In its 2018 “Statement on the Importance of Preserving Personal Privacy,” the ACM outlined a series of “Foundational Privacy Principles and Practices,” including:

Ensure that communications with individuals (i.e., data subjects) are comprehensible, readable, and straightforward.

Ensure that individuals are able to prevent personal data obtained for one purpose from being used or made available for other purposes without that person's informed consent.¹¹⁹

135. There's been a concerted multi-year effort by US companies to convince the world that regulations on data collection are unnecessary, and that regulation should only apply to data use. Many corporations and lobbyists seek to eradicate any limitations on data collection because they know that any use limitations would be narrowly defined, and could be slowly expanded over time.¹²⁰ These parties recognize that once collection limitations are in place, it will be much

¹¹⁸ Association for Computing Machinery, “ACM code of ethics and professional conduct,” <https://www.acm.org/code-of-ethics> (June 22, 2018).

¹¹⁹ Association for Computing Machinery, US Public Policy Council, “USACM statement on the importance of preserving personal privacy,” https://www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf (March 1, 2018).

¹²⁰ Craig Mundie, “Privacy pragmatism: Focus on data use, not data collection,” *Foreign Affairs* 93, <http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism> (March/April 2014).

William Hoffman, et al., “Rethinking personal data: Trust and context in user-centred data ecosystems,” World Economic Forum, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (May 2014).

William H. Dutton et al., “The Internet trust bubble: Global values, beliefs and practices,” World Economic Forum, http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf (May 2014).

Fred H. Cate, Peter Cullen, and Viktor Mayer-Schonberger, “Data protection principles for the 21st century: Revising the 1980 OECD Guidelines,” Oxford Internet Institute, University of Oxford, http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf (March 2014).

Rodriguez v. Google

harder to revise them. But as with government mass surveillance, the privacy harms proceed from the simple collection (and saving) of the data, not only from its use.¹²¹ Unrestricted data collection will result in large repositories of data, expansive sharing with the government and other third parties, and a slow deterioration of narrowly defined use restrictions.

5.3. There Are Many Privacy Risks Post-Collection

136. There are many post-collection risks to consumer privacy that proceed from the accumulation of user data. For example, malevolent actors, acting independently or under government direction, may access it and either exploit it themselves, or offer it for sale to others. Personally identifying information may be used for the purpose of identity theft.

137. As of February 2, 2023, Google's parent company Alphabet had 190,234 employees.¹²² Additionally, in 2019, Google employed 121,000 temporary employees and contractors.¹²³ Leaked internal documents indicate that between 2018 and 2020, Google fired 80 employees for abusing their access to the company's data, including mishandling confidential information, misusing the company's systems, and improperly accessing user data.¹²⁴ Like many organizations, Google has been forced to acknowledge numerous instances of sexual harassment by managers (some of whom were handsomely rewarded upon their departure from the company in spite of having victimized other employees).¹²⁵ In 2010, the company fired an engineer for accessing the Google accounts of four minors, including one who had tried to cut off communication with him,¹²⁶ and in 2014, a Google employee was arrested for cyberstalking.¹²⁷ It is to be expected that any large organization will have its share of staff who abuse their power, as well as those who can be coerced or bribed.

President's Council of Advisors on Science and Technology, "Big data and privacy: A technology perspective," http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (May 2014).

¹²¹ Chris Jay Hoofnagle, "The Potemkinism of privacy pragmatism," *Slate*, http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.html (September 2, 2014).

¹²² Alphabet, Inc., "Alphabet announces fourth quarter and FY 2022 results," https://abc.xyz/investor/static/pdf/2022Q4_alphabet_earnings_release.pdf (February 2, 2023).

¹²³ Daisuke Wakabayashi, "Google's shadow work force: Temps who outnumber full-time employees," *New York Times*, <https://www.nytimes.com/2019/05/28/technology/google-temp-workers.html> (May 28, 2019).

¹²⁴ Joseph Cox, "Leaked document says Google fired dozens of employees for data misuse," *VICE*, <https://www.vice.com/en/article/g5gk73/google-fired-dozens-for-data-misuse> (August 4, 2021).

¹²⁵ Jennifer Elias, "Google's \$310 million sexual harassment settlement aims to set new industry standards," *CNBC*, <https://www.cnbc.com/2020/09/29/googles-310-million-sexual-misconduct-settlement-details.html> (September 29, 2020).

Rosalie Chan and Hugh Langley, "Hundreds of Google employees call on company to change sexual-misconduct policies that they say put the burden on survivors," *Business Insider*, <https://www.businessinsider.com/google-employees-alphabet-union-petition-justice-for-jessica-misconduct-policies-2021-7> (July 21, 2021).

¹²⁶ Adrian Chen, "GCreep: Google engineer stalked teens, spied on chats (Updated)," *Gawker*, <https://www.gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats> (September 14, 2010).

¹²⁷ Erin Allday, "Google worker arrested for cyberstalking," *SFGate*, <https://www.sfgate.com/crime/article/Google-worker-arrested-for-cyberstalking-5848161.php> (October 25, 2014).

Rodriguez v. Google

138. User data can also be stolen at the behest of hostile governments. For example, in September 2017, the credit bureau Equifax announced that between May and July 2017, hackers had stolen personally identifying data of 147.9 million US citizens, as well as another 15 million citizens of the UK and Canada. The hack was facilitated by not just one, but three points of failure: the company's failure to patch a vulnerability in a dispute resolution portal, its failure to adequately segment its servers, and its storage of administrative credentials in plain text, rather than in encrypted form. After a two-and-a-half-year investigation, the FBI charged four members of the People's Republic of China's armed forces with the attack. Investigators suspect that the mainland Chinese government is working to gather information on US citizens in order to identify US government officials and intelligence operatives, and to pinpoint targets for bribery or blackmail.¹²⁸

139. In a 2020 interview, Google's UX Manager Kalle Buschmann correctly observed that "one of the most obvious [privacy] risks to actual users is oppressive governments and surveillance; use of mobile devices to aid in prosecution."¹²⁹

140. Courts may order the disclosure of user data subject to a subpoena, issued either at the behest of government actors (such as police and prosecutors), or parties to civil litigation.¹³⁰ Google's privacy policy notes this risk, stating that Google "will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosures of the information is reasonable necessary to: Meeting any applicable law, regulations, legal process, or enforceable governmental request."¹³¹

141. Datasets may also be merged, enabling the identification of individuals in spite of efforts to prevent this.

6. Privacy and System Design

6.1. People's Privacy Intuition Is Not Suited for the Internet

142. People reveal data about themselves all the time: to family, friends, acquaintances, lovers, even strangers. They share personal information with doctors, investment counselors, and psychologists. They share a lot of data. But they usually think of that sharing transactionally: "I'm sharing data with you, because I need you to know things/trust you with my secrets/am reciprocating because you've just told me something personal." That sharing usually occurs in

¹²⁸ Josh Fruhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?" *CSO Magazine*, <https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html> (February 12, 2020).

US Federal Bureau of Investigation, "Chinese military hackers charged in Equifax breach," <https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020> (February 10, 2020).

¹²⁹ GOOG-RDGZ-00188868 at -80.

¹³⁰ Jay Greene, "Tech giants have to hand over your data when federal investigators ask. Here's why," *Washington Post*, <https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation> (June 15, 2021).

¹³¹ Google, "Google privacy policy: Sharing your information," <https://policies.google.com/privacy?hl=en-US#infossharing> (February 10, 2022).

Rodriguez v. Google

the context of face-to-face encounters, in which people are typically in control and aware of what they are sharing.

143. People have evolved all sorts of psychological systems to navigate complex privacy decisions, systems that are themselves complex, highly attuned, and delicately social. A person may walk into a party and immediately know how to behave. Whom to talk to, what to tell to whom, who's in the vicinity, who's listening: most humans are equipped to navigate the social waters. Technology inhibits that ability, as most people relegated to socializing on Zoom during the COVID-19 pandemic can attest. Move our interactions into an online setting, and suddenly intuition begins to fail. People forget who's reading their posts. They accidentally send something private to a public forum. They don't understand how their data is monitored in the background. They don't realize what the technologies they're using can and cannot do.

144. Humans are social animals, and there are few things more powerful or rewarding to humans than communicating with other people. Digital means have become the easiest and quickest way to communicate; they have functioned as a lifeline for millions of people sequestered in their homes during the COVID-19 pandemic. However, trading privacy for services isn't necessarily a good or fair bargain, at least as these bargains are structured today, absent comprehensive federal legislation comparable to Europe's GDPR. Users have become too easily accustomed to accepting invidious deals presented in opaque, frequently modified privacy policies, and whose terms they do not fully understand (or worse yet, to being accused of consenting to data collection practices that were never disclosed at all).

145. Tracking of online behavior and mobile app usage is also largely invisible. Trackers do not announce themselves or make themselves apparent. Users are likely to be unaware of the many trackers that monitor their every move on their desktop machine or mobile phone, unless they install a browser extension like Privacy Badger, or apps like Exodus and uBlock Origin, which are designed to reveal that information.¹³² Nor would those users have insight into how their data is being saved and used. People shouldn't need to be technical experts, or learn and use complex developer tools, to understand what is going on. The sheer amount of Internet and mobile app surveillance just isn't apparent.

146. This lack of transparency makes it hard for people to make complex privacy decisions about the browsers they use, websites they visit, apps they install on their smartphones, and the amount of personal information they disclose via all of these means. Once people can't directly perceive other people, intuition fails and thoughts of privacy fade into the background. People don't think, "There's a multinational corporation recording everything I say and targeting me with advertising." People don't think, "The US and maybe other governments are recording everything I say and trying to find terrorists, or criminals, or drug dealers, or the Villain-of-the-Month." That's not obvious. What's obvious is, "I'm at this gathering, with my friends and acquaintances, and we're talking about personal stuff."

147. Users' continual exposure of their data online cannot serve as evidence of their consent to be monitored, especially when they seek to affirmatively protect their privacy using a privacy control like WAA or sWAA. People consent to the real-world analogue of social interaction and

¹³² PrivacyTools.io, "Exodus for Android: Finds trackers embedded in all your apps," <https://www.privacytools.io/guides/exodus-for-android-finds-trackers> (page accessed December 7, 2022).

Rodriguez v. Google

intellectual exploration that they have in their heads without fully understanding the ramifications of moving that model online.

6.2. Personal Data Is Difficult to Anonymize and Easy to De-anonymize

148. Maintaining anonymity against a ubiquitous surveillor is nearly impossible. If an Internet user forgets even once to enable privacy protections, or clicks on the wrong link, or types the wrong thing, they've permanently attached their name to whatever anonymous provider they're using. The level of operational security required to maintain privacy and anonymity in the face of a focused and determined investigation is beyond the resources of even trained government agents. Even a team of highly trained Israeli assassins was quickly identified in Dubai, based on surveillance camera footage from around the city.¹³³

149. The same is true for large sets of anonymous data. Users might naïvely think that there are so many users in the world that it's easy to hide in the sea of data. That's not true. Most techniques for anonymizing data don't work. Ostensibly anonymized data can be de-anonymized with surprisingly little information.¹³⁴ The details can be complicated and situation-dependent, but basically humans are surprisingly unique.

150. In 1997, computer scientist Latanya Sweeney—then an MIT graduate student—demonstrated that she could de-anonymize records by correlating birth dates and ZIP codes with the voter registration database.¹³⁵ Several years later, using publicly available, purportedly anonymous data from the 1990 census, Sweeney found that 87% of the population in the United States—216 million of 248 million people—could be uniquely identified by their five-digit ZIP code combined with their gender and date of birth.¹³⁶ Other researchers reported similar results using the 2000 census data.¹³⁷ Sweeney and her colleagues have extended her work on deanonymization to encompass the Personal Genome Project, hospitalization records, and environmental health studies.¹³⁸

¹³³ Ronen Bergman, et al, "An eye for an eye: The anatomy of Mossad's Dubai operation," *Der Spiegel*, <https://www.spiegel.de/international/world/an-eye-for-an-eye-the-anatomy-of-mossad-s-dubai-operation-a-739908.html> (January 17, 2011).

¹³⁴ Paul Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Review* 57, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (August 13, 2009).

¹³⁵ Latanya Sweeney, "Weaving technology and policy together to maintain confidentiality," *Journal of Law, Medicine and Ethics* 25, <http://onlinelibrary.wiley.com/doi/10.1111/j.1748-720X.1997.tb01885.x/abstract> (June 1997).

¹³⁶ Latanya Sweeney, "Simple demographics often identify people uniquely," Carnegie Mellon University Data Privacy Working Paper 3, <https://dataprivacylab.org/projects/identifiability/paper1.pdf> (2000).

¹³⁷ Philippe Golle, "Revisiting the uniqueness of simple demographics in the U.S. population," 5th ACM Workshop on Privacy in the Electronic Society (WPES'06), Alexandria, Virginia, <https://crypto.stanford.edu/~pgolle/papers/census.pdf> (October 30, 2006).

¹³⁸ Latanya Sweeney, Akua Abu and Julia Winn, "Identifying participants in the Personal Genome Project by name (A re-identification experiment)," arxiv.org, <https://arxiv.org/abs/1304.7605> (2013).

Latanya Sweeney, "Only you, your doctor, and many others may know," *Technology Science* 2018, <https://techscience.org/a/2015092903> (September 28, 2015).

Rodriguez v. Google

151. In 2006, AOL released three months of search data for 657,000 users: 20 million searches in all. The idea was that it would be useful for researchers; to protect people's identity, they replaced names with numbers. So, for example, Bruce Schneier might be 608429. AOL was surprised when researchers were able to attach names to numbers by correlating different items in individuals' search history.¹³⁹

152. In 2008, Netflix published 10 million movie rankings by 500,000 anonymized customers, as part of a challenge for people to come up with better recommendation systems than the one the company was using at that time. Researchers were able to de-anonymize those customers by comparing rankings and time stamps with public rankings and time stamps in the Internet Movie Database.¹⁴⁰

153. A 2015 study of three months' worth of credit card metadata generated by 1.1 million people found that four spatiotemporal points were sufficient to uniquely re-identify 90% of individuals.¹⁴¹

154. One 2019 study found that 99.98% of Americans could be correctly re-identified in any purportedly anonymized dataset using fifteen demographic attributes, and that even in incomplete datasets, individuals could be re-identified.¹⁴²

155. A 2018 study from Vanderbilt University explored the extent and magnitude of Google's collection of data on individual users, and demonstrated anew the ease with which supposedly anonymized data could be identified. The authors established that mobile advertising identifiers could be de-anonymized by means of data sent to Google via passing of device-level identification information to Google servers by an Android device, and that DoubleClick cookie IDs, which record user activity on third-party web pages, could be connected with a user's Google account if a user accessed a Google application using the same browser holding the DoubleClick cookie. From the study:

“In step 1, a “checkin” data is sent to the URL `android.clients.google.com/checkin`. This particular communication provides an Android data sync to Google servers and contains Android log information (e.g. recovery log), kernel messages, crash dumps, and other device-related identifiers.... Through the checkin process, Android sends to Google a

Ji Su Yoo, et al., “Risks to patient privacy: A re-identification of patients in Maine and Vermont statewide hospital data,” *Technology Science* 2018, <https://techscience.org/a/2018100901> (October 8, 2018).

Katherine E. Boronow, et al., “Privacy risks of sharing data from environmental health studies,” *Environmental Health Perspectives* 128, no. 1, <https://ehp.niehs.nih.gov/doi/10.1289/EHP4817> (January 2020).

¹³⁹ Michael Barbaro and Tom Zeller Jr., “A face is exposed for AOL Search No. 4417749,” *New York Times*, <http://www.nytimes.com/2006/08/09/technology/09aol.html> (August 9, 2006).

¹⁴⁰ Arvind Narayanan and Vitaly Shmatikov, “Robust de-anonymization of large sparse datasets,” 2008 IEEE Symposium on Security and Privacy, Oakland, California, <https://web.stanford.edu/class/cs245/win2020/readings/netflix-deanonymization.pdf> (May 18-20, 2008).

¹⁴¹ Yves-Alexandre de Montjoye, et al., “Unique in the shopping mall: On the re-identifiability of credit card metadata,” *Science* 347, no. 6221, <https://www.science.org/doi/full/10.1126/science.1256297> (January 30, 2015).

¹⁴² Luc Rocher, Julien M. Jendrickx and Yves-Alexandre de Montjoye, “Estimating the success of re-identifications in incomplete datasets using generative models,” *Nature Communications* 10, <https://www.nature.com/articles/s41467-019-10933-3> (July 23, 2019).

Rodriguez v. Google

variety of important device-related permanent identifiers, including device MAC address, IMEI /MEID, and device serial number. Moreover, these requests also contain the Android user's Gmail ID. The data present in checkin uploads enable Google to connect a user's personal information with Android device permanent identifiers.

"In step 2, the reply to the checkin request comes from the Google server. This message contains a Google services framework identifier (GSF ID) that is similar to the actual "Android ID."

"Step 3 entails another instance of communication where the same GSF ID (from step 2) is sent to Google together with the GAID."

"Through the above three data exchanges, Google receives the information needed to connect a GAID with permanent device identifiers as well as users' Google Account IDs. These intercepted data exchanges with Google servers from an Android phone show how Google can connect anonymized information collected on an Android mobile device via DoubleClick, Analytics or AdMob tools with the user's personal identity."¹⁴³

156. Another study, from 2020, found that anonymized user location data could be combined with anonymized credit card data to identify specific individuals.¹⁴⁴ A 2021 study demonstrated means by which sensitive information about minor students could be ascertained by linking anonymized datasets to publicly available school data.¹⁴⁵

157. These might seem like special cases, but they're not. It is not difficult to correlate anonymized data with identified data. Someone with access to an anonymized data set of telephone records, for example, might partially de-anonymize it by correlating it with a catalog merchant's telephone order database. Amazon's online book reviews could be the key to partially de-anonymizing a database of credit card purchase details.

158. A 2019 research paper built a model to estimate how easy it would be to de-anonymize an arbitrary dataset. They found that in most cases it was easy, and concluded: "Our results reject the claims that, first, re-identification is not a practical risk and, second, sampling or releasing partial datasets provide plausible deniability. Moving forward, they question whether current de-identification practices satisfy the anonymization standards of modern data protection laws such as GDPR and CCPA and emphasize the need to move, from a legal and regulatory perspective, beyond the de-identification release-and-forget model."¹⁴⁶ In other words, anonymization doesn't work as a privacy preserving tool.

¹⁴³ Douglas C. Schmidt, et al., "Google data collection," Vanderbilt University, <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf> (August 15, 2018).

¹⁴⁴ Dániel Kondor, et al., "Towards matching user mobility traces in large-scale datasets," arXiv:1709.05772, <https://arxiv.org/pdf/1709.05772.pdf> (August 13, 2018).

¹⁴⁵ Eli Yacobson, et al., "De-identification is insufficient to protect student privacy, or What can a field trip reveal?" *Journal of Learning Analytics* 8, no 2, <https://www.learning-analytics.info/index.php/JLA/article/view/7353> (2021).

¹⁴⁶ Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Communications* 10, article 3069, <https://www.nature.com/articles/s41467-019-10933-3> (July 23, 2019).

Rodriguez v. Google

159. Nonetheless, de-anonymization can be used for benevolent purposes. A 2021 paper describes a technique designed to ferret out fraudulent Google Play store reviews and the professional search rank workers who post them, by associating Google Play user accounts with user accounts on sites offering search rank fraud jobs, then analyzing the activity within the accounts.¹⁴⁷

6.3. The Industry Uses Dark Patterns to Nudge Users in Particular Directions

160. Much user interface design consists of norms and metaphors that people develop to make sense of what computers do under the hood. The metaphors are just that: files, folders, trashcans, and directories are to all some extent abstractions and representations. And they're not always accurate. When we move a file into a folder, we're not actually moving anything, just changing a pointer designating where the file is stored. Deleting a file isn't the same thing as destroying the physical object, something that prosecutors, defendants and their attorneys learn over and over again as files they thought they'd deleted (or redacted) are recovered and used against them. But they're close enough for most purposes. And the norms are taken from the real world as much as possible.¹⁴⁸

161. "Dark patterns" is an umbrella term for a variety of subversive user-design tricks intended to manipulate users into doing things they wouldn't normally choose to do. The term was coined in 2010 by cognitive scientist and user-interface researcher Harry Brignull to describe ways in which user-interface designers "take our understanding of human psychology and flip it over to the dark side."¹⁴⁹ By this, he meant that while many online user interfaces "are carefully crafted with a solid understanding of human psychology," they "do not have the user's interests in mind."¹⁵⁰ Dark patterns co-opt common design elements to steer users towards certain ends, including forfeiting their privacy unawares.

162. In the physical world, commonly understood design elements are used to guide people through public activities associated with risk to life, liberty or property. Driving, for example, is regulated by use of a trusted visual language: green means go, and red means stop. The Internet, by comparison, has grown so quickly, so profitably, and with so little regulation, that norms of ethical design have only begun to evolve in retrospect, in response to increasingly widespread practices by online entrepreneurs seeking to extract revenue from their users.¹⁵¹

163. While green and red are also used as guides in online user experience design all the time, they become a dark pattern when the guidance that "green means go" established by a series of

¹⁴⁷ Mizanur Rahman, et al., "Towards de-anonymization of Google Play search rank fraud," *IEEE Transactions on Knowledge and Data Engineering* 33, no. 11, <https://ieeexplore.ieee.org/document/9003210> (November 2021).

¹⁴⁸ Bruce Schneier, *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back*, WW Norton & Co, 2023.

¹⁴⁹ Harry Brignull, "Dark patterns: Deception vs. honesty in web design," *A List Apart*, <https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design> (November 1, 2011).

¹⁵⁰ Harry Brignull, "Dark patterns: Inside the interfaces designed to trick you," *The Verge*, <http://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you> (August 29, 2013).

¹⁵¹ Trine Falbe, Kim Andersen and Martin Michael Frederiksen, *White Hat UX: The Next Generation in User Experience*, pej gruppens forlag, <https://www.smashingmagazine.com/printed-books/white-hat-ux> (April 10, 2017).

Rodriguez v. Google

green “continue” buttons is suddenly subverted to sell an in-app purchase, as in the mobile game “Two Dots.”¹⁵² Or when ads for software unrelated to the site being viewed place a green “click here to download” button as they interrupt a series of “continue” buttons in a sequence of web pages. Way too often buttons like these cause the user to download something other than what they were expecting.

164. Examples of dark patterns are everywhere online. An investigation by ProPublica found that Intuit, the developer of TurboTax, has a free tax filing program called Free File for users who make less than a certain amount per year. But many users are tricked into paying for the tax filing features in TurboTax by a user interface design that intentionally makes it difficult to find and use the free version.¹⁵³ Amazon uses a dark pattern to prevent users from canceling their accounts: it takes independent research, then at least five hard-to-find clicks, and finally a chat with customer service.¹⁵⁴ The Donald J. Trump campaign has used dark patterns to trick supporters into contributing far more money than they had intended; for example, fundraising solicitations featured pre-checked boxes authorizing weekly recurring and bonus donations, with the opt-out box obscured beneath screens of text and a fine-print disclaimer.¹⁵⁵ The cleverest example? A banner ad from a company called Chatmost that has what looks a speck of dust on a touchscreen, tricking users into clicking on the ad as they try to swipe away the dirty spot.¹⁵⁶

165. Dark patterns are common on smartphone apps. One 2020 study examined 240 popular apps and found one or more dark patterns on 95% of them, with the average app incorporating seven different deceptive user interface elements.¹⁵⁷ A 2021 study “found that they [users] are generally aware of the influence that manipulative designs can exert on their online behaviour. However, being aware does not equip users with the ability to oppose such influence.”¹⁵⁸

166. Brignull’s original typology of dark patterns included trick questions, sneaking unwanted items into a basket or unwanted features into a service, misdirection, and bait and switch. User interface designer and Purdue University professor Colin Gray has extended the scholarship on dark patterns, and defines them similarly: “instances where designers use their knowledge of

¹⁵² Gila Lyons, “An ode to Two Dots, the game that eases my anxious mind,” *VICE*, https://www.vice.com/en_us/article/zmkdea/two-dots-iphone-game-anxiety-stress-relief-sleep (September 5, 2018).

¹⁵³ Ariana Tobin, Justin Elliott and Meg Marco, “Here are your stories of being tricked into paying by TurboTax. You often need the money,” *ProPublica*, <https://www.propublica.org/article/here-are-your-stories-of-being-tricked-into-paying-by-turbotax-you-often-need-the-money> (April 26, 2019).

ProPublica, “The TurboTax trap (Series index),” <https://www.propublica.org/series/the-turbotax-trap> (accessed February 20, 2023).

¹⁵⁴ Elsie Otachi, “How to delete an Amazon account,” *Help Desk Geek*, <https://helpdeskgeek.com/how-to/how-to-delete-an-amazon-account> (August 11, 2020).

¹⁵⁵ Shane Goldmacher, “How Trump steered supporters into unwitting donations,” *New York Times*, <https://www.nytimes.com/2021/04/03/us/politics/trump-donations.html> (April 3, 2021).

¹⁵⁶ Nerdwriter, “How dark patterns trick you online,” YouTube, <https://youtu.be/kxkrdLI6e6M> (March 28, 2018).






¹⁵⁷ Linda Di Geronimo, et al., “UI dark patterns and where to find them: A study of mobile applications and user perception,” CHI ‘20, April 25–30, 2020, Honolulu, HI, USA, <https://dl.acm.org/doi/pdf/10.1145/3313831.3376600> (April 2020).

¹⁵⁸ Kerstin Bongard-Blanchy, et al., “‘I am definitely manipulated, even when I am aware of it. It’s ridiculous!’—Dark patterns from the end-user perspective,” ACM DIS Conference on Designing Interactive Systems, <https://orbilu.uni.lu/handle/10993/47008> (June 28–July 2, 2021).

Rodriguez v. Google

human behavior (e.g., psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest."¹⁵⁹ In a 2018 paper, Gray and colleagues identified five broad categories of dark patterns that they understand to encompass the whole space:

- **Nagging** constitutes the “redirection of expected functionality that persists beyond one or more interactions.”
- **Obstruction** makes a process more difficult than it needs to be, so that users will simply give up.
- **Sneaking** involves withholding or concealing relevant information so that users will choose products and services that they do not really want.
- **Interface interference** makes it easier for users to make choices that benefit the person controlling the interface.
- **Forced action** involves requiring users to do something they wouldn't ordinarily do in order to obtain something or some functionality that they want.¹⁶⁰

 <p>NAGGING</p> <p>Redirection of expected functionality that persists beyond one or more interactions.</p>	 <p>OBSTRUCTION</p> <p>Making a process more difficult than it needs to be, with the intent of dissuading certain action(s).</p> <p>INCLUDES: Brignull "Roach Motel," "Price Comparison Prevention," and Intermediate Currency</p>	 <p>SNEAKING</p> <p>Attempting to hide, disguise, or delay the divulging of information that is relevant to the user.</p> <p>INCLUDES: Brignull "Forced Continuity," "Hidden Costs," "Sneak into Basket," and "Bait and Switch"</p>	 <p>INTERFACE INTERFERENCE</p> <p>Manipulation of the user interface that privileges certain actions over others.</p> <p>INCLUDES: Hidden Information, Preselection, Aesthetic Manipulation, Toying with Emotion, False Hierarchy, Brignull "Disguised Ad," and "Trick Questions"</p>	 <p>FORCED ACTION</p> <p>Requiring the user to perform a certain action to access (or continue to access) certain functionality.</p> <p>INCLUDES: Social Pyramid, Brignull "Privacy Zuckering," and Gamification</p>
---	---	--	---	---

167. The 2017 book *White Hat UX* lists twelve different dark patterns: bait and switch, disguised ads, forced continuity, forced disclosure, friend spam, misdirection, road block, roach motel, door slam, trick questions, clickbait, and hidden costs.¹⁶¹ These can be mapped to Gray's taxonomy.

168. The EU Data Protection Board states that the use of dark patterns can violate both data protection regulations and consumer protection regulations because they can “lead users into making unintended, unwilling and potentially harmful decisions in regards of their personal data.” The Board's taxonomy delineates six broad patterns:

¹⁵⁹ Colin M. Gray, et al., “The dark (patterns) side of UX design,” CHI 2018, Montreal, Quebec, Canada, <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (April 21-26, 2018).

¹⁶⁰ Colin M. Gray, et al., “The dark (patterns) side of UX design,” CHI 2018, Montreal, Quebec, Canada, <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (April 21-26, 2018).

¹⁶¹ Trine Falbe, Kim Andersen and Martin Michael Frederiksen, *White Hat UX: The Next Generation in User Experience*, pej gruppens forlag, <https://www.smashingmagazine.com/printed-books/white-hat-ux> (April 10, 2017).

Rodriguez v. Google

- **Overloading**, when “users are confronted with an avalanche/large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of the data subject.”
- **Skipping**, or “designing the interface or user experience in a way that users forget or do not think about all or some of the data protection aspects.”
- **Stirring**, which “affects the choice users would make by appealing to their emotions or using visual nudges.”
- **Hindering**, or “obstructing or blocking users in their process of becoming informed or managing their data by making the action hard or impossible to achieve.”
- **Fickle**, when “the design of the interface is inconsistent and not clear, making it hard for the user to navigate the different data protection control tools and to understand the purpose of the processing.”
- **Left in the dark**, which “means an interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights.”¹⁶²

169. Computer scientist Arvind Narayanan describes the economic, moral and psychological harms that can ensue from the use of dark patterns: “Dark patterns enable designers to extract three main resources from users: money, data, and attention.... The most obvious way is simply to nudge (or trick) consumers into spending more than they otherwise would. A less obvious, yet equally pervasive, goal of dark patterns is to invade privacy.... A third goal of dark patterns is to make services addictive.”¹⁶³ Ryan Calo of the University of Washington School of Law adds “autonomy harm” to this list, reasoning that vulnerable users have less control over their own behavior than they might were they not being unethically manipulated by the developers of sites they visit and apps they use.¹⁶⁴

170. David Martin of the European Consumer Organization adds to this list of harms the potential for dark patterns to give rise to emotional or psychological distress, by invoking guilt over a particular choice, fear of being cheated or missing out on an opportunity, or other manifestations of emotional pressure; and the potential for dark patterns to waste users’ time by deliberately making privacy-protective choices arduous.¹⁶⁵

¹⁶² Andrea Jelinek, et al., “Dark patterns in social media platform interfaces: How to recognise and avoid them,” Version 1.0, European Data Protection Board, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (14 March 2022).

¹⁶³ Arvind Narayanan, et al., “Dark patterns: Past, present and future,” *ACM Queue* 18, no. 2, <https://queue.acm.org/detail.cfm?id=3400901&doi=10.1145%2F3400899.3400901> (May 17, 2020).

¹⁶⁴ Ryan Calo, “Digital market manipulation,” *George Washington Law Review* 82, no. 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703 (August 2014).

¹⁶⁵ David Martin, “Dark patterns: Impact on consumers and potential harm,” Public Hearing, Committee on the Internal Market and Consumer Protection, <https://www.europarl.europa.eu/cmsdata/246802/BEUC%20PPT%20Dark%20Patterns%20Hearing%20IMCO-16%20March%202022.pdf> (March 16, 2022).

Rodriguez v. Google

171. Regulators in both Europe and the US have sought to regulate the most egregiously deceptive aspects of dark patterns by means of the EU General Data Protection Regulation¹⁶⁶ and Digital Services Act,¹⁶⁷ California Consumer Privacy Act,¹⁶⁸ and the Colorado Privacy Act.¹⁶⁹

172. In 2019, US senators Mark Warner and Deb Fischer introduced legislation that would ban dark patterns.¹⁷⁰ The senators, joined by four of their colleagues, reintroduced it in 2021.¹⁷¹ If passed, the DETOUR Act—for “Deceptive Experiences To Online Users Reduction”—would:

- Prohibit large online operators from designing, modifying, or manipulating user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data.
- Prohibit subdividing or segmenting consumers for the purposes of behavioral experiments without a consumer’s informed consent, which cannot be buried in a general contract or service agreement. This includes routine disclosures for large online operators, not less than once every 90 days, on any behavioral or psychological experiments to users and the public. Additionally, the bill would require large online operators to create an internal Independent Review Board to provide oversight on these practices to safeguard consumer welfare.
- Prohibit user design intended to create compulsive usage among children under the age of 13 years old (as currently defined by the Children’s Online Privacy Protection Act).
- Direct the FTC to create rules within one year of enactment to carry out the requirements related to informed consent, Independent Review Boards, and professional standards bodies.¹⁷²

173. A September 2022 FTC report on dark patterns and their harms described deceptive design elements in e-commerce interfaces, cookie consent banners and popups, children’s apps, and subscription sales. Four categories of particular interest to the FTC included:

- Design elements that induce false beliefs, such as misleading consumers by disguising ads as editorial rather than commercial content;

¹⁶⁶ European Union, “General data protection regulation (GDPR),” <https://gdpr-info.eu> (April 27, 2016).

¹⁶⁷ European Commission, “The Digital Services Act package,” <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (November 24, 2022).

¹⁶⁸ Office of the Attorney General, “California Consumer Privacy Act,” <https://oag.ca.gov/privacy/ccpa> (accessed December 19, 2022).

¹⁶⁹ Colorado Legislature, “Senate Bill 21-90: Colorado Privacy Act,” https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf (enacted July 7, 2021)

¹⁷⁰ Mark R. Warner, “Senators introduce bipartisan legislation to ban manipulative ‘dark patterns’,” Office of Mark R. Warner, <https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns> (April 9, 2019)

¹⁷¹ Mark R. Warner, “Lawmakers announce additional support for bipartisan, bicameral legislation to ban manipulative ‘dark patterns,’” Office of Mark R. Warner, <https://www.warner.senate.gov/public/index.cfm/2022/6/lawmakers-announce-additional-support-for-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns> (June 15, 2022).

¹⁷² Mark R. Warner, “Lawmakers reintroduce bipartisan bicameral legislation to ban manipulative ‘dark patterns,’” Office of Mark R. Warner, <https://www.warner.senate.gov/public/index.cfm/2021/12/lawmakers-reintroduce-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns> (December 8, 2021).

Rodriguez v. Google

- Design elements that lead to unauthorized charges, such as making it difficult to cancel subscriptions or recurring charges;
- Design elements that hide or delay disclosure of material information, such as burying key terms and junk fees in small print, mouseover text and dense TOS policies; and
- Design elements that obscure or subvert privacy choices, such as tricking consumers into sharing data.¹⁷³

174. Well before publication of this report, the FTC had ramped up its efforts to combat the deception of online consumers using visual tricks and misdirection:

- In April 2020, rent-to-own payment plan company Progressive Leasing was fined \$175 million to settle charges that it had misled consumers about the cost of its services, hiding the full cost of their payment plans in a screen accessible only via a small dropdown arrow labeled simply “Additional Lease Details.”¹⁷⁴
- In July 2021, online lender Lending Club Corporation agreed to pay \$18 million for falsely advertising that its loan services came with “no hidden fees,” when in fact fees were hidden inside of tooltips that did not need to be clicked on and viewed in order to continue filling out the loan application.¹⁷⁵
- In March 2022, the FTC sued Intuit for falsely advertising its tax filing services as “free, free, free,” but failing to notify users of their ineligibility for free services until after they entered all of their personal and income information into the program and arrived at a subscription upgrade page. The portal to TurboTax’s Free File program did not appear on the TurboTax website, but under a completely different URL, taxfreedom.com.¹⁷⁶
- In September 2022, the FTC filed a complaint against credit monitoring company Credit Karma for misrepresenting that consumers were “pre-approved” for credit cards, when in fact nearly a third of applicants were denied. The company’s web pages touting “pre-approved” lines of credit were developed with the aid of A/B testing, which found that consumers were more likely to click on their advertisements if they included the word

¹⁷³ US Federal Trade Commission, “Bringing dark patterns to light,” Staff Report, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (September 2022).

¹⁷⁴ US Federal Trade Commission, “Rent-to-own payment plan company Progressive Leasing will pay \$175 million to settle FTC charges it deceived consumers about pricing,” <https://www.ftc.gov/news-events/news/press-releases/2020/04/rent-own-payment-plan-company-progressive-leasing-will-pay-175-million-settle-ftc-charges-it> (April 20, 2020).

¹⁷⁵ US Federal Trade Commission, “Complaint,” *FTC v. Lending Club Corporation*, Case 3:18-cv-02454, https://www.ftc.gov/system/files/documents/cases/lending_club_complaint.pdf (filed April 25, 2018).

US Federal Trade Commission, “LendingClub agrees to pay \$18 million to settle FTC charges,” <https://www.ftc.gov/news-events/news/press-releases/2021/07/lendingclub-agrees-pay-18-million-settle-ftc-charges> (July 24, 2021).

¹⁷⁶ US Federal Trade Commission, “FTC sues Intuit for its deceptive TurboTax “free” filing campaign,” <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-sues-intuit-its-deceptive-turbotax-free-filing-campaign> (March 29, 2022).

Justin Elliott and Lucas Waldron, “Here’s how TurboTax just tricked you into paying to file your taxes,” *Pro Publica*, <https://www.propublica.org/article/turbotax-just-tricked-you-into-paying-to-file-your-taxes> (April 22, 2019).

Rodriguez v. Google

“pre-approved” than if they stated that the applicant had “excellent” odds of being approved.¹⁷⁷

- In November 2022, Internet service provider Vonage entered into an agreement with the FTC to pay over \$100 million for forcing users to jump through numerous hoops to cancel their contacts. One of these hoops involved locating the company’s customer service phone number, which was not made readily available on the website.¹⁷⁸
- In December 2022, Fortnite developer Epic Games, Inc., entered into an agreement with the FTC to pay a total of \$520 million over allegations that the company violated the Children’s Online Privacy Protection Act (COPPA) by implementing privacy-invasive on-by-default text and voice communications settings, and making the controls for turning them off difficult to find. Additional dark patterns served “to dupe millions of players into making unintentional purchases.” These included confusing configurations of buttons and other controls, and allowing purchases to be made with the press of a single button rather than requiring confirmation.¹⁷⁹

175. Other federal agencies, as well as state Attorneys General, have taken assertive steps to counter deception of consumers by dark patterns:

- In March 2022, online travel agency Fareportal entered into a \$2.6 million agreement with the office of the New York Attorney General, following allegations that it had misled customers by means of “dark patterns” embedded on its website. For example:
 - When consumers searched for flights, the Fareportal site would display messages falsely stating the number of tickets left for the most popular flights. If a consumer searched for one ticket, they would be warned that only two were left; if two, then three, and so on.
 - Similar tactics were used for hotel accommodations; messages displaying the number of rooms available, or the proportion of available rooms already booked, did not correspond to reality, but to the consumer’s search.
 - The popularity of travel insurance and seat upgrades, and the number of users currently viewing the same flight or hotel listing, were also represented inaccurately, with computer-generated random numbers substituting for nonexistent real-time data.
 - Countdown timers were misleadingly used to create a false sense of urgency.¹⁸⁰

¹⁷⁷ US Federal Trade Commission, “FTC takes action to stop Credit Karma from tricking consumers with allegedly false ‘pre-approved’ credit offers,” <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-takes-action-stop-credit-karma-tricking-consumers-allegedly-false-pre-approved-credit-offers> (September 1, 2022).

¹⁷⁸ US Federal Trade Commission, “FTC action against Vonage results in \$100 million to customers trapped by illegal dark patterns and junk fees when trying to cancel service,” <https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-action-against-vonage-results-100-million-customers-trapped-illegal-dark-patterns-junk-fees-when-trying-cancel-service> (November 3, 2022).

¹⁷⁹ US Federal Trade Commission, “Fortnite video game maker Epic Games to pay more than half a billion dollars over FTC allegations of privacy violations and unwanted charges,” <https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations> (December 19, 2022).

¹⁸⁰ Office of the Attorney General, “Attorney General James secures \$2.6 million from online travel agency for deceptive marketing,” <https://ag.ny.gov/press-release/2022/attorney-general-james-secures-26-million-online-travel-agency-deceptive> (March 16, 2022).

Rodriguez v. Google

- In April 2022, the Consumer Finance Protection Bureau sued credit services firm TransUnion, alleging that the company had willfully violated a 2017 agreement to refrain from deceptive advertising practices. CFPB asserted that “TransUnion asked consumers to provide credit card information that appeared to be part of an identity verification process. TransUnion then integrated deceptive buttons into the online interface that gave the impression that the consumer could also access a free credit score in addition to viewing their free credit report. In reality, clicking this button signed consumers up for recurring monthly charges using the credit card information they had provided. The only indication in the enrollment process that consumers were making some sort of purchase was through a fine print, low contrast disclosure, located off to the side of the enrollment form. The disclosure is inside an image that can take up to 30 seconds longer to load than the rest of the material in the form.”¹⁸¹
- In May 2022, Intuit reached a settlement with the attorneys general of all fifty states and the District of Columbia, agreeing to pay \$141 million in restitution to 4.4 million low-income customers who were misled by the company’s deceptive software design into paying for tax preparation services they were originally led to believe would be free.¹⁸² (The FTC complaint mentioned above is a separate action.)

176. The use of dark patterns violates the above-cited ACM Code of Ethics¹⁸³:

Dark user experience (UX) patterns, which are designs that intend to trick users toward unintended (and often more expensive) options, cause harm. They can make users feel duped (Principle 1.2), provide deliberately misleading information (Principle 1.3), or discriminate against those with disabilities (Principle 1.4). Computing professionals have a moral obligation to use their skills to benefit the members of society (Principle 1.1), not to deceive them. Furthermore, the use of dark UX patterns is an affront to the dignity of users, violating Principle 2.1. Consequently, dark UX patterns violate several of the core principles of the Code.¹⁸⁴

177. Google’s extensive use of dark patterns is discussed in Section 9.4. Google’s use of dark patterns with respect to WAA is discussed in Section 11.

¹⁸¹ Consumer Financial Protection Bureau, “CFPB charges TransUnion and senior executive John Danaher with violating law enforcement order,” <https://www.consumerfinance.gov/about-us/newsroom/cfpb-charges-transunion-and-senior-executive-john-danaher-with-violating-law-enforcement-order> (April 12, 2022).

¹⁸² Greg Iacurci, “TurboTax owner Intuit to pay \$141 million to customers ‘unfairly charged,’” CNBC, <https://www.cnbc.com/2022/05/04/turbotax-owner-intuit-to-pay-141-million-to-customers.html> (May 4, 2022).

US Federal Trade Commission, “Notice of settlement with state Attorneys General,” *In the matter of Intuit Inc.*, Federal Trade Commission Office of Administrative Law Judges Docket No. 94-9, https://www.ftc.gov/system/files/ftc_gov/pdf/D09408%20-%20NOTICE%20OF%20SETTLEMENT%20WITH%20STATE%20ATTORNEYS%20GENERAL%20-%20PUBLIC%20%281%29.pdf (May 5, 2022).

¹⁸³ Association for Computing Machinery, “ACM code of ethics and professional conduct,” <https://www.acm.org/code-of-ethics> (June 22, 2018).

¹⁸⁴ Association for Computing Machinery, “Case: Dark UX patterns,” <https://ethics.acm.org/code-of-ethics/using-the-code/case-dark-ux-patterns> (July 10, 2018).

V. Google-Specific Topics

7. Google's Surveillance-Dependent Business Model

7.1. Google Makes Money from Harvesting User Data

178. There is a conflict between the Google's desire for data and its users' desire for privacy. Users want control over their privacy. At the same time, Google's business model demands the maximization of data collection, and creates a strong incentive to overpromise and underdeliver on privacy. In February 2023, Google's parent company Alphabet announced FY 2022 revenues of \$282.836 billion.¹⁸⁵ This revenue stream is derived from the vast amount of personal information Google collects about people.

179. Google's mission statement asserts that the company's goal is "to organize the world's information and make it universally accessible and useful,"¹⁸⁶ and the company has pursued that goal through its search engine. However, this mission statement obscures the fact that the preponderance of Google's revenue is derived from advertising. For the 2022 fiscal year, Google reported \$224 billion in advertising revenue, representing a 79% share of revenue from advertising.¹⁸⁷

180. Originally, Google's advertisements were displayed according to the content of searches, but with the expansion of services to include SDKs embedded within non-Google websites and apps, the company was able to capitalize on the information accumulated about the online activity of users of those third-party websites and apps. Google's ability to track and analyze individual users' web and app activity has enabled it to create even more comprehensive user profiles than those afforded by search alone; the expanded ability to capture data across many domains, including from users' activity on non-Google domains, not only from Google users but from users of apps that use Google services, enables Google to provide more granular user information to advertisers, who pay a premium to more effectively target their desired audiences.¹⁸⁸

181. Google gathers, organizes and monetizes a range of personal data that is far more comprehensive than generally recognized. In its product description on the Apple App Store, Google states that its Chrome browser app collects the following information linked to users' identities:

- Location: Coarse Location
- Search History
- Browsing History

¹⁸⁵ Alphabet, Inc., "Alphabet announces fourth quarter and FY 2022 results," https://abc.xyz/investor/static/pdf/2022Q4_alphabet_earnings_release.pdf (February 2, 2023).

¹⁸⁶ Google, "About Google," <https://about.google> (accessed February 20, 2023).

¹⁸⁷ Alphabet, Inc., "Form 10-K," United States Securities and Exchange Commission, https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf?cache=5ae4398 (February 3, 2023).

¹⁸⁸ Megan Graham and Jennifer Elias, "How Google's \$150 billion advertising business works," CNBC, <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html> (May 18, 2021).

Rodriguez v. Google

- Identifiers: User ID, Device ID
- Usage Data: Product Interaction
- Diagnostics: Performance Data, Other Diagnostic Data
- Other Data: Other Data Types
- Financial Info: Payment Info
- Contact Info: Physical Address, Email Address, Name, Phone Number
- Contacts
- User Content: Photos or Videos, Audio Data, Other User Content¹⁸⁹

182. Other Google apps on the Apple App Store gather a similarly broad range of personal and device data. Google Meet, Google Photos, Google Classroom, Google Drive, and Gmail all use coarse location, contacts and search history for analytics purposes.¹⁹⁰ Google Home and Google Maps use both search history and browsing history for third-party advertising and analytics.¹⁹¹ YouTube uses location, search, and browsing history for both first- and third-party advertising, and location and search history for analytics.¹⁹²

183. Software libraries included with the Firebase SDK enable Google to collect data from people using non-Google apps, including information such as the user's age bracket, gender and interests, that can be used by both Google and developers who use Google Analytics for Firebase to understand their user base:

- Age: The age of the user by bracket: 18-24, 25-34, 35-44, 45-54, 55-64, and 65+.
- App store: The store from which the app was downloaded and installed.
- App version: The versionName (Android) or the Bundle version (iOS).
- Browser: The browser from which user activity originated.
- City: The city from which user activity originated.
- Continent: The continent from which user activity originated.

¹⁸⁹ Google, "Google Chrome," <https://apps.apple.com/us/app/google-chrome/id535886823> (accessed February 20, 2023).

¹⁹⁰ Google, "Google Meet," Apple App Store, <https://apps.apple.com/us/app/google-meet/id1096918571> (accessed January 12, 2023).

Google, "Google Photos," Apple App Store, <https://apps.apple.com/us/app/google-classroom/id924620788> (accessed January 12, 2023).

Google, "Google Classroom," Apple App Store, <https://apps.apple.com/us/app/google-classroom/id924620788> (accessed January 12, 2023).

Google, "Google Drive," Apple App Store, <https://apps.apple.com/us/app/google-drive/id507874739> (accessed January 12, 2023).

Google, "Gmail," Apple App Store, <https://apps.apple.com/us/app/gmail-email-by-google/id422689480> (accessed January 12, 2023).

¹⁹¹ Google, "Google Home," Apple App Store, <https://apps.apple.com/us/app/google-home/id680819774> (accessed January 12, 2023).

Google, "Google Maps," Apple App Store, <https://apps.apple.com/us/app/google-maps/id585027354> (accessed January 12, 2023).

¹⁹² Google, "YouTube," Apple App Store, <https://apps.apple.com/us/app/youtube-watch-listen-stream/id544007664> (accessed January 12, 2023).

Rodriguez v. Google

- Country: The country from which user activity originated.
- Device brand: The brand name of the mobile device (such as Motorola, LG, or Samsung).
- Device category: The category of the mobile device (such as mobile or tablet).
- Device model: The mobile device model name (such as iPhone 5s or SM-J500M).
- Gender: The gender of the user (male or female).
- Interests: The interests of the user (such as Arts & Entertainment, Games, Sports).
- Language: The language setting of the device OS (such as en-us or pt-br).
- New/Established: New: First opened the app within the last 7 days; Established: First opened the app more than 7 days ago.
- Operating system: The operating system used by visitors to your website or mobile app.
- OS version: The operating system version used by visitors to your website or mobile app (such as 9.3.2 or 5.1.1).
- Platform: The platform on which your website or mobile app ran (such as web, iOS, or Android).
- Region: The geographic region from which user activity originated.
- Subcontinent: The subcontinent from which user activity originated.¹⁹³

184. Google collects a similar range of data through AdMob: age, app store, app version, country, device brand, device category, device model, gender, interests, language, new/established, and OS version, as well as the time the user first opens the app.¹⁹⁴

185. Another Google service that enables Google to serve and monetize advertisements on non-Google apps is Google Ad Manager.¹⁹⁵ Apps that wish to use Google AdMob or Ad Manager can do so by embedding within their apps the Google Mobile Ads SDK. As with AdMob, Ad Manager enables Google to collect data about users' activity on non-Google apps, including ad impressions and ad clicks.¹⁹⁶

186. In mobile apps, Google uses Google Analytics to derive "demographic and interest data" from the Android Advertising ID (AdID, introduced in 2014¹⁹⁷) and the iOS Identifier for Advertisers (IDFA, introduced in 2012¹⁹⁸).¹⁹⁹ These are unique IDs assigned to individual

¹⁹³ Google, "[GA4] Predefined user dimensions," *Analytics Help*, <https://support.google.com/firebase/answer/9268042> (accessed December 21, 2022).

¹⁹⁴ Google, "Automatically collected user properties," *Google AdMob Help*, <https://support.google.com/admob/answer/9755590?hl=en> (accessed January 27, 2023).

¹⁹⁵ Google, "Overview of apps with Ad Manager," *Google Ad Manager Help*, <https://support.google.com/admanager/answer/6238688?hl=en> (accessed February 11, 2023).

¹⁹⁶ Google, "Counting impressions and clicks," *Google Ad Manager Help*, <https://support.google.com/admanager/answer/2521337?hl=en> (accessed February 11, 2023).

¹⁹⁷ Jim Edwards, "Google's new 'Advertising ID' is now live and tracking Android phones: This is what it looks like," *Business Insider*, <https://www.businessinsider.com/googles-new-advertising-id-is-now-live-and-tracking-new-android-phonesthis-is-what-it-looks-like-2014-1> (January 27, 2014).

¹⁹⁸ Jim Edwards, "Apple has quietly started tracking iPhone users again, and it's tricky to opt out," *Business Insider*, <https://www.businessinsider.com/ifa-apples-iphone-tracking-in-ios-6-2012-10> (October 11, 2012).

¹⁹⁹ Google, "[GA4] Demographic details report," *Analytics Help*, <https://support.google.com/analytics/answer/12948931> (accessed February 11, 2023).

Rodriguez v. Google

devices that, when linked to demographic and interest data, enable ads personalization and cross-device targeting.

187. Both iOS and Android enable users to delete their device's AdID or IDFA.²⁰⁰ The effectiveness of such controls, however, is far from assured. A 2021 study of Apple's App Tracking Transparency (ATT) control, which purports to give users the opportunity to disable third-party tracking by blocking access to their smartphone's IDFA, found that ATT "made no difference in the total number of active third-party trackers, and had a minimal impact on the total number of third-party tracking connection attempts.... [D]etailed personal or device data was being sent to trackers in almost all cases."²⁰¹

188. Given the scale at which Google operates, and the extraordinary range of information that the company accumulates about its users, Google's data collection practices (including its collection of data from users who have disabled WAA or sWAA) can be characterized as a form of pervasive monitoring; that is, "widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers.... [Pervasive monitoring] is distinguished by being indiscriminate and very large scale... [Pervasive monitoring] is an attack on the privacy of Internet users and organisations."²⁰²

7.2. Google Search Has an Overwhelming Market Share

189. Google was founded in 1998 as a search engine. Although it was originally one among many, the turn of the twenty-first century saw Google rise to the top of the heap, thanks to its comprehensive web crawling and superior search results.

190. In their 1998 paper "The anatomy of a large-scale hypertextual web search engine," Google founders Sergey Brin and Larry Page warned of the potential impact of advertising on their invention:

Currently, the predominant business model for commercial search engines is advertising. **The goals of the advertising business model do not always correspond to providing quality search to users.** For example, in our prototype search engine one of the top results for cellular phone is "The Effect of Cellular Phone Use Upon Driver Attention", a study which explains in great detail the distractions and risk associated with conversing on a cell phone while driving. This search result came up first because of its high importance as judged by the PageRank algorithm, an approximation of citation importance on the web [Page, 98]. It is clear that a search engine which was taking money for showing cellular phone ads would have difficulty justifying the page that

²⁰⁰ Bennett Cyphers, "How to disable ad ID tracking on iOS and Android, and why you should do it now," Electronic Frontier Foundation, <https://www EFF.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now> (May 11, 2022).

²⁰¹ Johnny Lin and Sean Halloran, "Study: Effectiveness of Apple's App Tracking Transparency," *Transparency Matters*, <https://blog.lockdownprivacy.com/2021/09/22/study-effectiveness-of-apples-app-tracking-transparency.html> (September 22, 2021).

²⁰² Stephen Farrell and Hannes Tschofenig, "Pervasive monitoring is an attack," *Best Current Practice* 188, Internet Engineering Task Force, (May 2014).

our system returned to its paying advertisers. For this type of reason and historical experience with other media [Bagdikian 83], **we expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers.**

Since it is very difficult even for experts to evaluate search engines, search engine bias is particularly insidious. A good example was OpenText, which was reported to be selling companies the right to be listed at the top of the search results for particular queries [Marchiori 97]. This type of bias is much more insidious than advertising, because it is not clear who “deserves” to be there, and who is willing to pay money to be listed. This business model resulted in an uproar, and OpenText has ceased to be a viable search engine. But less blatant bias are likely to be tolerated by the market. For example, a search engine could add a small factor to search results from “friendly” companies, and subtract a factor from results from competitors. This type of bias is very difficult to detect but could still have a significant effect on the market. Furthermore, advertising income often provides an incentive to provide poor quality search results. For example, we noticed a major search engine would not return a large airline’s homepage when the airline’s name was given as a query. It so happened that the airline had placed an expensive ad, linked to the query that was its name. A better search engine would not have required this ad, and possibly resulted in the loss of the revenue from the airline to the search engine. In general, it could be argued from the consumer point of view that the better the search engine is, the fewer advertisements will be needed for the consumer to find what they want. This of course erodes the advertising supported business model of the existing search engines. However, there will always be money from advertisers who want a customer to switch products, or have something that is genuinely new. But **we believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm.**²⁰³ [*emphasis added*]

191. Google was once the sort of transparent, academic service that its founders envisioned; however, since its discovery that user-generated data could be monetized, Google has evolved into the world’s largest and most multifaceted commercial mechanism for mass surveillance.

192. Google Search, in contrast to some competing search engines, collects information from users, including IP address, user agent, cookie IDs, queries, and clicks. The value of this information creates an incentive for Google to ensure that users turn to the Google Search app as the “entry point” of their online activities.

193. The Google Chrome web browser debuted in 2008, and was made available at no monetary cost to users. In a 2012 interview, Google CEO Sundar Pichai noted that Chrome’s profitability lay in the fact that it could run on all platforms, and that by developing its own

²⁰³ Sergey Brin and Lawrence Page, “The anatomy of a large-scale hypertextual web search engine,” *Computer Networks and ISDN Systems* 30, no. 1-7, <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/334.pdf> (April 1998).

Rodriguez v. Google

browser, Google reduced the necessity of sharing revenue with other browsers that people might use to run Google searches. Google Search, he stated, contributed the greatest proportion of Google's revenue; users who search the web via Google see ads on the search engine, then proceed to websites hosting Google-enabled display ads.²⁰⁴

194. As of November 2022, Google had an 83.78% share of the global desktop search engine market,²⁰⁵ and a 96% share of the mobile search engine market.²⁰⁶ Although the company doesn't disclose its exact search volume data, it has been estimated that Google processes over 20 petabytes of data every day, including approximately 63,000 search queries per second, which amounts to 3.5–5.6 billion search queries per day.²⁰⁷

195. In August 2020, Google entered into a three-year deal with Mozilla, agreeing to pay \$300–\$350 million dollars for Google Search to remain the default search engine for Firefox—a privilege that carries with it the right to serve advertisements to those Firefox users who don't switch to other search providers.²⁰⁸ The Oslo, Norway-based browser Opera has had a similar “search distribution agreement” with Google since 2001.²⁰⁹ The privacy-focused browser Brave had a similar arrangement with Google until August 2021, when it introduced its own search engine.²¹⁰

196. Industry analysts estimated in 2018 that the cost of Google's annual search distribution agreement with Apple, which made Google Search the default search engine on all Apple products, was between \$7 billion and \$10 billion.²¹¹ Apple is reportedly developing its own

²⁰⁴ Stephen Shankland, “Sundar Pichai: Chrome ‘exceptionally profitable’ for Google (q&a),” *CNET*, <https://www.cnet.com/tech/services-and-software/sundar-pichai-chrome-exceptionally-profitable-for-google-q-a> (June 29, 2012).

²⁰⁵ Statcounter, “Desktop search engine market share worldwide,” <https://gs.statcounter.com/search-engine-market-share/desktop/worldwide> (accessed December 21, 2022).

²⁰⁶ Statcounter, “Mobile search engine market share worldwide, November 2021–November 2022,” <https://gs.statcounter.com/search-engine-market-share/mobile/worldwide> (accessed December 21, 2022).

²⁰⁷ Seed Scientific, “How much data is created every day?” <https://seedscientific.com/how-much-data-is-created-every-day> (October 28, 2021).

Meg Prater, “25 Google search statistics to bookmark ASAP,” *HubSpot*, <https://blog.hubspot.com/marketing/google-search-statistics> (June 9, 2021).

²⁰⁸ Matthew Humphries, “Mozilla signs lucrative 3-year Google search deal for Firefox,” *PC Magazine*, <https://www.pcmag.com/news/mozilla-signs-lucrative-3-year-google-search-deal-for-firefox> (August 14, 2020).

²⁰⁹ Opera Limited, “Opera and Google renew search agreement,” *PR Newswire*, <https://www.prnewswire.com/news-releases/opera-and-google-renew-search-agreement-301448072.html> (December 20, 2021).

²¹⁰ Jon Porter, “Brave browser replaces Google with its own search engine,” *The Verge*, <https://www.theverge.com/2021/10/20/22736142/brave-browser-search-engine-default-google-quant-duckduckgo-web-discovery-project> (October 20, 2021).

²¹¹ Peter Cao, “Google reportedly paying Apple \$9 billion to remain default search engine in Safari on iOS,” *9to5 Mac*, <https://9to5mac.com/2018/09/28/google-paying-apple-9-billion-default-search-engine> (September 28, 2018).

Ben Lovejoy, “Google paid Apple almost \$10 billion in 2018, ‘Apple Prime’ service needed in 2019 says Goldman Sachs,” *9to5 Mac*, <https://9to5mac.com/2019/02/12/google-paid-apple-prime-service> (February 12, 2019).

Eric Savitz, “Apple should buy a search engine, analyst says,” *Barron's*, <https://www.barrons.com/articles/amazon-stock-split-51646863502> (June 8, 2020).

Rodriguez v. Google

search engine, and is increasingly providing its own search function for selected applications on its devices.²¹² The payments from Google have nonetheless continued; in August 2021, analysts reported that Google’s payment to Apple would rise to \$15 billion in 2021, and to between \$18 billion and \$20 billion in 2022.²¹³

7.3. Google’s Android OS Dominates the Global Smartphone Market

197. The Android mobile device operating system was purchased by Google in 2005, and first brought to market under license to HTC Corporation in 2008.²¹⁴ Since that time, Android has grown to hold a 72% share of the global mobile market; in the US (home to Apple and its many devotees), it holds a 44% share.²¹⁵

198. As Android’s share of the global mobile operating system market has grown, so too has the market share of Google apps that must be pre-installed on devices running Android in order for developers to comply with the various agreements that make up the Android license. Such requirements dramatically increase the pool of users from whom the data fueling Google’s advertising business is extracted.

199. In July 2018, the European Union’s Executive Commission levied a €4.34 billion fine against Google for anticompetitive behavior, particularly its practice of “giving” Android to mobile device makers, with strings attached.²¹⁶ The Commission charged that Google had run afoul of the law, in part, by requiring manufacturers to pre-install the Google Search app and Chrome browser app as a condition for licensing Google’s Play Store. Although Google had argued that it needed to enforce these conditions in order to monetize its investment in Android, the Commission noted that “Google achieves billions of dollars in annual revenues with the Google Play Store alone, it collects a lot of data that is valuable to Google’s search and advertising business from Android devices, and it would still have benefitted from a significant

²¹² Tim Bradshaw and Patrick McGee, “Apple develops alternative to Google search,” *Financial Times*, <https://www.ft.com/content/fd311801-e863-41fe-82cf-3d98c4c47e26> (October 28, 2020).

²¹³ Chance Miller, “Analysts: Google to pay Apple \$15 billion to remain default Safari search engine in 2021,” *9to5Mac*, <https://9to5mac.com/2021/08/25/analysts-google-to-pay-apple-15-billion-to-remain-default-safari-search-engine-in-2021> (August 25, 2021).

²¹⁴ Christian de Looper and Daniel Martin, “From Android 1.0 to Android 10, here’s how Google’s OS evolved over a decade,” *Digital Trends*, <https://www.digitaltrends.com/mobile/android-version-history> (March 30, 2021).

²¹⁵ Statcounter, “Mobile operating system market share worldwide, Nov 2021—Nov 2022,” <https://gs.statcounter.com/os-market-share/mobile/worldwide> (accessed December 28, 2022).

Statcounter, “Mobile operating system market share United States of America, Nov 2021—Nov 2022,” <https://gs.statcounter.com/os-market-share/mobile/united-states-of-america> (accessed December 28, 2022).

²¹⁶ Adam Satariano and Jack Nicas, “E.U. fines Google \$5.1 billion in Android antitrust case,” *New York Times*, <https://www.nytimes.com/2018/07/18/technology/google-eu-android-fine.html> (July 18, 2018).

Rodriguez v. Google

stream of revenue from search advertising without the restrictions.”²¹⁷ The decision was recently upheld, with some modifications, upon appeal.²¹⁸

200. In October 2022, the Competition Commission of India fined Google \$162 million after concluding that the company’s requirement that device manufacturers pre-install and prominently display the full Google Mobile Suite if they wanted to license Android at all represented “imposition of unfair condition on the device manufacturers,” and therefore violated India’s Competition Act.²¹⁹ In a press release announcing its ruling, the Commission noted that, “Google’s business was found to be driven by the ultimate intent of increasing users on its platforms so that they interact with its revenue earning service, i.e., online search which directly affects sale of online advertising services by Google.” The Commission found that Google’s multiple agreements governing developers’ use of Android served to lock in a competitive advantage not only with respect to the operating system, but to the default search app and search engine, and “another revenue earning app, i.e. YouTube.”²²⁰ From the Commission’s order:

The Commission notes that to determine relevant turnover in relation to technology platforms, such as one operated by Google, it is important to appreciate the business model, incentives of the platforms and their revenue streams. Various products of Google work on the basis of network effects i.e., with the increase in numbers of users on its platform, the attractiveness of the platform/ products for the advertisers increases multi-fold. In such platforms, not only two/ multi sides are intricately intertwined and interwoven with each other, but the products/ services offered by the platform operator (Google in this case) derive strength from each other due to economies of scope and scale. Replicating such an ecosystem becomes extremely difficult for a new entrant. Competition in such a scenario is amongst ecosystems and not just the verticals or independent services. In such a case, the entire platform has to be taken as one unit to account for the cross-market externalities between platform sides, and revenue generated therefrom has to be seen as a whole.

...Google’s core products include, a web browser (Google Chrome), an online video streaming service (YouTube), a web-based e-mail service (Gmail), an online mapping, navigation and geolocation service (Google Maps), an app store (Play Store), etc. These services are part of Google Mobile Services

²¹⁷ European Commission, “Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google’s search engine,” https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581 (July 18, 2018).

²¹⁸ Natasha Lomas, “Google fails to overturn EUJ’s €4BN+ Android antitrust decision,” *Tech Crunch*, <https://techcrunch.com/2022/09/14/google-eu-android-antitrust-appeal-ruling> (September 14, 2022).

²¹⁹ Manish Singh, “India fines Google \$162 million for anti-competitive practices on Android,” *Tech Crunch*, <https://techcrunch.com/2022/10/20/india-fines-google-162-million-for-anti-competitive-practices-on-android> (October 20, 2022).

²²⁰ Competition Commission of India, “CCI imposes a monetary penalty of Rs. 1337.76 crore on Google for anti-competitive practices in relation to Android mobile devices,” <https://www.cci.gov.in/antitrust/press-release/details/261/0> (October 20, 2022).

Rodriguez v. Google

(GMS) i.e., the bundle of Google apps and services that Google licenses to smartphone manufacturers/Original Equipment Manufacturers (OEMs).

...The Commission notes that most of these products are offered for free to users and primarily monetized through advertising revenue for Google. The foregoing analysis as well as financial details clearly reflect the singularity and focus of Google on advertising, in its business operations. Google Play is also an important cog in this wheel where it generates more revenues through advertising rather than through service fee.²²¹

201. In October 2014, Google announced its acquisition of Firebase, a set of software libraries that developers can use to incorporate functionality into their apps that they might not otherwise be able to provide.²²² Google has since then expanded Firebase to include a suite of mobile back-end services, including analytics, messaging, authentication, database creation, file storage, crash reporting, performance evaluation, and ad placement and reporting.

202. The Firebase SDK has enabled Google's collection of data generated during users' interactions with apps. By January 2023, 93% of Android apps using analytics SDKs integrated Firebase; 88% of Android apps using ad network SDKs integrated Google AdMob (which makes use of Firebase).²²³

7.4. It Is Practically Impossible to Avoid Using Google Products and Services

203. From its headquarters in California, Google has established massive data centers around the world to power its search engine, email, and data storage operations, and to accumulate and organize the information submitted and generated by users that powers its advertising operations.

204. Gmail reportedly has 1.8 billion users world-wide, comprising 30% of all email clients. This includes 61% of all 18-28-year-olds. Three-quarters of those users access their email on mobile devices.²²⁴

205. More than one billion people use Google Maps every month. Over five million apps and websites incorporate Google Maps into their offerings.²²⁵

²²¹ Competition Commission of India, "Order under Section 27 of the Competition Act, 2002," *In re Alphabet Inc., Google LLC, etc.*, <https://www.cci.gov.in/antitrust/orders/details/1072/0>.

²²² James Tamplin, "Firebase is joining Google!" *The Firebase Blog*, <https://firebase.blog/posts/2014/10/firebase-is-joining-google> (October 21, 2014).

²²³ 42 Matters, "Top 15 analytics SDKs used in Android apps," <https://42matters.com/sdk-analysis/top-analytics-sdks> (last updated January 12, 2023).

42 Matters, "Top 20 ad network SDKs used in Android apps," <https://42matters.com/sdk-analysis/top-ad-network-sdks> (last updated January 12, 2023).

²²⁴ Litmus, "Email client market share in April 2022," <https://www.litmus.com/blog/email-client-market-share-april-2022> (April 2022).

²²⁵ Ethan Russell, "9 things to know about Google's maps data: Beyond the map," *Google Cloud Blog*, <https://cloud.google.com/blog/products/maps-platform/9-things-know-about-googles-maps-data-beyond-map> (September 30, 2019).

Rodriguez v. Google

206. Firebase is incorporated into many of the world’s most-used apps, including Alibaba, the New York Times, Twitch.tv, Lyft, Instacart, Venmo, and National Public Radio.²²⁶ As of October 2020, over 2.5 million active apps used Firebase.²²⁷ According to mobile intelligence firm MightySignal, as of July 2022, Firebase was installed in 462,633 apps; as of November 2022, Firebase had captured 90% of the app platform SDK market.²²⁸

207. There is no way to completely avoid Google. In 2020, security journalist Kashmir Hill verified this by trying to validate assertions made by the chief executives of the largest technology companies in testimony before Congress, assuring legislators that consumers have numerous options for the services that they provide. She failed. Hill noted that:

“Amazon and Google were the hardest companies to avoid by far.... When I blocked Google, the entire Internet slowed down for me, because almost every site I visited was using Google to supply its fonts, run its ads, track its users, or determine if its users were humans or bots. While blocking Google, I couldn’t sign into the data storage service Dropbox because the site thought I wasn’t a real person. Uber and Lyft stopped working for me, because they were both dependent on Google Maps for navigating the world. I discovered that Google Maps had a de facto monopoly on online maps. Even Google’s longtime critic Yelp used it to tell computer users where businesses could be found. I came to think of Amazon and Google as so embedded in the architecture of the digital world that even their competitors had to rely on their services.”

208. Recalling tech companies’ glib advice, “If you don’t like the company, don’t use its products,” Hill concluded that “it’s not possible to do that. It’s not just the products and services branded with the big tech giant’s name. It’s that these companies control a thicket of more obscure products and services that are hard to untangle from tools we rely on for everything we do, from work to getting from point A to point B.” After her experiment was over, Hill “went back to using the companies’ services again, because as it demonstrated, I didn’t really have any other choice.”²²⁹

7.5. Google Collects Data About Users’ Interactions with Non-Google Websites and Apps

209. Google collects data from users’ activity on non-Google websites and apps by way of a variety of Google services. Google Ads (formerly, Google AdWords, its original advertising product, long-familiar to users of Google Search), AdMob (its mass-market tool for in-app ads), AdSense (for publishers who want a quick and easy way to place ads on their sites and earn income), Ad Manager (formerly DoubleClick for Publishers, for high-end mobile app developers and website publishers who sell advertising on their own platforms), Google Analytics (for website owners to understand user engagement), and Google Analytics for Firebase (for app

²²⁶ Ajavi Abimbola Samuel, “Top 10 big companies using Firebase,” *Career Karma*, <https://career Karma.com/blog/companies-that-use-firebase> (February 10, 2022).

²²⁷ GOOG-RDGZ-00061878 at -81.

²²⁸ Mighty Signal, “Firebase Android SDK,” <https://mightysignal.com/sdk/android/1432/firebase> (accessed December 2, 2022).

²²⁹ Kashmir Hill, “I tried to live without the tech giants. It was impossible,” *New York Times*, <https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html> (July 31, 2020).

Rodriguez v. Google

developers). In 2018, over 1.1 million Android apps used Google’s ad software, a figure that has surely risen over the years.²³⁰ One 2020 study found that visitors to 86% of the world’s 50,000 most-visited websites contained Google trackers;²³¹ another put the figure at 87%;²³² and yet another found Google trackers on 80.3% of websites globally, and 79.5% of websites in the United States.²³³

210. In January 2012, Google announced its intent to combine information collected from all Google services, couching the plan as a way to do “cool things” that benefit users. Although users were assured that the move would result in “sharing more of your information with...well, you,”²³⁴ the years that followed saw an unprecedented rise in the extent to which Google collected, saved, and exploited that user information to create astonishingly intimate profiles of its users’ demographics, financial status, interests, and habits.

211. Google’s data collection is enabled in large part to Google’s provision of Google Analytics free of charge to websites with less than ten million hits per month, and also with Google providing Google Analytics for Firebase free of charge to app developers. According to an internal Google document, “Firebase has significant adoption among top developers,” including 74% of the top 1,000 Android apps.²³⁵

212. Although Google claims not to sell users’ data, Google transmits sensitive user data, including geolocation, device IDs, unique cookies containing identifiers, and browsing information, to sell advertising space through ad auctions in a process known as “real-time bidding” (RTB).²³⁶

213. The ad auction process is exceedingly complex and beyond the scope of this report. However, a 2018 analysis of the then-potential impact of GDPR on online advertising by the Interactive Advertising Bureau, an industry standards-setting body, noted that the proposed

²³⁰ Paresh Dave, “Google’s app network quietly becomes huge growth engine,” Reuters, <https://www.reuters.com/article/idUSKCN1FZ0F9> (February 15, 2018).

²³¹ John Koetsier, “Google is tracking you on 86% of the top 50,000 websites on the planet,” *Forbes*, <https://www.forbes.com/sites/johnkoetsier/2020/03/11/google-is-tracking-you-on-86-of-the-top-50000-websites-on-the-planet> (March 11, 2020).

²³² Geoffrey Fowler, “87 percent of websites are tracking you,” *Washington Post*, <https://www.washingtonpost.com/technology/2020/09/25/privacy-check-blacklight> (September 25, 2020).

²³³ Elaine Christie, “Tracking the trackers 2020: Web tracking’s opaque business model of selling users,” *Ghostery Blog*, <https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users> (2020).

²³⁴ Alma Whitten, “Updating our privacy policies and terms of service,” *Google Official Blog*, <https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html> (January 24, 2012).

²³⁵ GOOG-RDGZ-00070506 at -10.

²³⁶ Bennett Cyphers, “Google says it doesn’t ‘sell’ your data. Here’s how the company shares, monetizes, and exploits it,” Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and> (March 19, 2020).

Ethan Baron, “Google selling users’ personal data despite promise, federal court lawsuit claims,” *Tampa Bay Times*, <https://www.tampabay.com/news/2021/05/07/google-selling-users-personal-data-despite-promise-federal-court-lawsuit-claims> (May 7, 2021).

Rodriguez v. Google

regulation would require website owners and app developers to give users “prior information as to the identity of the data controller processing his or her personal data and the purposes of the processing.” However, they acknowledged that “it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding scenario,” which renders prior notice and consent impossible.²³⁷ A recent study by the Irish Council for Civil Liberties calls the RTB system the “biggest data breach ever recorded,” and reports that the average US citizen “has their online activity and location exposed 747 times every day” via RTB data transmissions.²³⁸

214. Google Analytics and Google Analytics for Firebase collect a wide range of data from users of websites and apps that employ it. Event-level data—that is, data about users’ activity on an app or website—enables developers and proprietors to understand their customers and potential customers, conduct their business operations, and monitor the effectiveness of their products.²³⁹ With this data, Google possesses an unprecedented level of knowledge about those users. Google:

- tracks text that a user types into a site or app’s search box or form, whether or not they perform the search or submit the form;
- tracks results of user searches within a site or app, and which search links the user clicks through;
- tracks videos a user watches within a site or app and for how long;
- tracks files a user downloads within a site or app.

215. Some corporate privacy officers have begun to question the wisdom of using Google Analytics because of Google’s retention of individual user data for its advertising enterprise, and the difficulty of obtaining truly informed consent from users who are not fully apprised of the specific data they are being asked to share.²⁴⁰

8. User Risks Caused by Google’s Data Collection

8.1. Users Face Risks from Joinability of Disparate Google Data Sets

216. Google employees in this case have referred to the data at issue as “pseudonymous” data.²⁴¹ As discussed in Section 6.2, the term is effectively meaningless. Google tellingly uses

²³⁷ IAB Europe, “The EU’s proposed new cookie rules 1: digital advertising, European media, and consumer access to online news, other content and services,” <https://brave.com/static-assets/files/1b-IAB-2017-paper.pdf> (November 20, 2018).

²³⁸ Johnny Ryan, “The biggest data breach,” Irish Council for Civil Liberties, <https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf> (May 16, 2022).

²³⁹ Google, “[GA4] Automatically collected events,” *Analytics Help*, https://support.google.com/analytics/answer/9234069?hl=en&ref_topic=9756175 (accessed December 21, 2022).

Google, “[GA4] Enhanced event measurement,” *Analytics Help*, <https://support.google.com/analytics/answer/9216061> (accessed December 21, 2022).

²⁴⁰ Maciej Zawadzinski, “The case against Google Analytics for organizations collecting personal data,” *CPO Magazine*, <https://www.cpomagazine.com/data-privacy/the-case-against-google-analytics-for-organizations-collecting-personal-data> (September 1, 2020).

²⁴¹ *E.g.*, Ganem Tr. 153:25-154:5.

Rodriguez v. Google

the term “pseudonymous” because “pseudonymized” data is far from anonymous. As astutely summarized by Eric Miraglia, Senior Director of Product Management at Google and the founder of Google’s Privacy and Data Protection Office: “We would use ‘anonymous’ to refer to data that cannot be tied to a data subject whereas pseudonymous data, in some cases, may be.”²⁴² Mr. Miraglia continued: “Pseudonymity is usually—usually referring to data that has not been mathematically anonymized. And so there’s always at least the hypothetical possibility of reidentification.”²⁴³ Google’s use of the term “pseudonymous” is effectively an admission that the data in question can be joined to users’ identifies, even if in isolation it is not explicitly linked to a person’s name.

217. By means of the Firebase SDK, Google “collects identifiers for mobile devices”, including “Android Advertising ID [AdID] and Advertising identifier [IDFA, or Identifier for Advertisers] for iOS.”²⁴⁴ Google will also receive “an app-instance identifier to identify a unique installation of the App.”²⁴⁵ While Google considers AdID, IDFA and app-instance identifiers to be pseudonymous, each of these identifies user data as coming from a specific device (and therefore the owner of that device). Google itself creates and controls so-called “pseudonymous” identifiers (e.g., AdID).²⁴⁶ Google uses its identifiers to track individual users across the apps they use, including by using AdID to track the impact of an advertisement on user behavior.²⁴⁷

218. Google employees have specifically admitted that “pseudonymous” data generated with WAA “off” can be linked to users and their Google Account, notwithstanding that Google calls it “pseudonymous.” For example, the authors of an internal 2019 draft product requirements document noted that “Currently for users with Web App and Activity control (WAA) off, we log to Zweiback. The expectation is that since these user queries are written to archival logs, these should not contain PII. This is problematic as these logs could potentially contain personal information which can lead to the undesirable outcome of anonymous logs having a potential join risk to personal Logs.”²⁴⁸ In a 2020 Privacy Working Group “Analytics Playbook,” Google software engineer Xinyu Ye noted that “ID joinability has been one of the biggest challenges in Google Analytics since introduction of GAIA IDs [the internal identifier at Google that identifies an account with an individual ²⁴⁹] in GA [Google Analytics].”²⁵⁰ In a September 2020 email written after this lawsuit was filed, Mr. Ye offered one example of a Firebase “joinability risk”: “Create the ability to link app events collected by GA4F [Google Analytics for Firebase] to GAIA ID even if end users turn off WAA and developers/customers disable Data sharing.”²⁵¹ Mr. Ye specifically identified a “subpoena” where Google would need “to retrieve Android

²⁴² Miraglia Tr. 106:16-107:1.

²⁴³ Miraglia Tr. 107:7-13.

²⁴⁴ GOOG-RDGZ-00100625.

²⁴⁵ GOOG-RDGZ-00100625.

²⁴⁶ GOOG-RDGZ-00056142 at -157 (informing app developers that “3P identifiers are not owned by you – these include advertising IDs like ... Google’s AdID”).

²⁴⁷ Langner Tr. 49:16-21, 185:13-17.

²⁴⁸ GOOG-RDGZ-00014556 at -58.

²⁴⁹ Ruemmler Tr. 74:13-14.

²⁵⁰ GOOG-RDGZ-00181801 at -08.

²⁵¹ GOOG-RDGZ-00033244.

Rodriguez v. Google

ADID data, app_instance_id data given a GAIA ID for users turning off WAA.”²⁵² Dan Stone, a Senior Product Manager working on Google Analytics, responded to Mr. Ye: “Can we update this to clarify that this is really expanding the ability, not creating it?”²⁵³ Google Analytics Group Product Manager Steve Ganem, who was also on this email thread, acknowledged during his deposition in this case that these “joinability risks” exist. While Mr. Ganem testified that Google has sometimes undertaken efforts to “reduce the joinability risks” it identified, it has not eliminated them entirely.²⁵⁴ Joinability risks will exist as long as Google collects pseudonymous data.

219. I agree with these Google employees’ observations regarding the joinability risk of this “WAA off” data. As I explained in Section 6.2, “Most techniques for anonymizing data don’t work. Ostensibly anonymized data can be de-anonymized with surprisingly little information.” Here, Google is not even trying to anonymize the data. Instead, Google stores the data with a “pseudonymous” identifier, which can be tied to the user’s identity.

220. The joinability risk is a byproduct of how Google saves data and uses that data to make money. For Google, saving data means linking data to certain identifiers. Google associates data with identifiers in order to benefit its advertising business, including for conversion tracking—that is, to measure the impact that an ad has on a user who sees it.

221. Even when WAA is off, Google is saving data from users’ online activity in a way that Google then uses for its own financial benefit. For example, Steve Ganem testified that Google “use[s] IDFA and ADID for conversion tracking even when WAA is off.” He elaborated that Google Analytics will match the identifiers collected “when a user clicks on an ad” to identifiers collected when the user “convert[s],” meaning performs some other action that the advertiser sought to encourage.²⁵⁵ Google calls device-based identifiers like ADID and IDFA “pseudonymous,” even though it uses these identifiers to track how individual users behave after being shown an advertisement.²⁵⁶ Google tracks users based on the data and identifiers that sit in so-called “pseudonymous logs.”²⁵⁷ Google is not only saving WAA-off data (in these logs, with these identifiers) but also using that data for its own enrichment.

8.2. Google Has a History of Data Breaches

222. Google’s decision to collect and save WAA-off data puts users at risk, particularly given the long history of data breaches targeting Google.

223. In late 2009, hackers from the People’s Republic of China exploited an intercept system Google had incorporated into Gmail in order to comply with US government surveillance requests. Malware installed on Google’s systems communicated with a server configured to receive exfiltrated data from Google and at least thirty-three other organizations. According to

²⁵² GOOG-RDGZ-00033244.

²⁵³ GOOG-RDGZ-00033245.

²⁵⁴ Ganem Tr. 259:20-260:9.

²⁵⁵ Ganem Tr. 251:14-15; 251:20-25.

²⁵⁶ Ganem Tr. 251:14-252:16.

²⁵⁷ Ganem Tr. 251:14-252:16.

Rodriguez v. Google

Google, the hackers sought access to the Gmail accounts of human rights activists focused on the PRC. Further investigation revealed that the attack, dubbed “Aurora,” was a state-sponsored counterespionage operation.²⁵⁸

224. In September 2014, a list of five million Gmail addresses and passwords was published on a Russian-language Bitcoin forum. Although Google claimed to have found no indication that its systems had been compromised, all listed accounts were locked, and users attempting to sign in were redirected to Google’s Account Recovery page.²⁵⁹

225. In October 2018, the *Wall Street Journal* reported that private user data from the Google+ social network had been accessible to outside developers for three years, from 2015 to 2018; vulnerable data included 500,000 users’ full names, email addresses, birth dates, gender, profile photos, places lived, occupation and relationship status. Outside developers using Google’s application programming interface (API) were also able to access user data designated as nonpublic, including their friends’ profiles.

226. In 2020, Awake Security uncovered hundreds of malicious Chrome extensions available on the Chrome Web Store that were capable of taking screenshots, reading a user’s clipboard, harvesting credential tokens, and recording user keystrokes (including passwords). All of these extensions were associated with a single registrar, GalComm. Google subsequently worked with the researchers to remove these extensions; it is nonetheless concerning that Google allowed them to be distributed on the Chrome Web Store in the first place.²⁶⁰

227. In 2019, security researchers discovered that the TikTok app bypassed safeguards built into the Android operating system in order to collect users’ unique mobile device identifiers (the MAC address) so that it could surreptitiously track them online, regardless of their privacy choices. Google banned the practice after discovering it.²⁶¹ Evidence was later found that TikTok was “able to avoid code audits on the Apple and Google app stores. [TikTok] is capable of

²⁵⁸ Kim Zetter, “Google hackers targeted source code of more than 30 companies,” *Wired*, <https://www.wired.com/2010/01/google-hack-attack> (January 13, 2010).

Mathew J. Schwartz, “Google Aurora hack was Chinese counterespionage operation,” *Dark Reading*, <https://www.darkreading.com/attacks-breaches/google-aurora-hack-was-chinese-counterespionage-operation> (May 21, 2013).

²⁵⁹ Jose Pagliery, “5 million Gmail passwords leaked,” CNN Business, <https://money.cnn.com/2014/09/10/technology/security/gmail-hack/index.html> (September 10, 2014).

²⁶⁰ Awake Security, “The internet’s new arms dealers: Malicious domain registrars,” <https://awakesecurity.com/blog/the-internets-new-arms-dealers-malicious-domain-registrars> (June 16, 2020).

²⁶¹ Kevin Poulsen and Robert McMillan, “TikTok tracked user data using tactic banned by Google,” *Wall Street Journal*, <https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738> (August 11, 2020).

Joel Reardon, et al., “50 ways to leak your data: An exploration of apps’ circumvention of the Android permissions system,” PrivacyCon 2019, Washington, D.C., https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf (June 27, 2019).

Rodriguez v. Google

changing the app’s behavior as it pleases without users’ knowledge and utilizes device tracking that essentially gives the company and third parties an all-access pass to user data.”²⁶²

228. In 2020, security researchers identified a vulnerability affecting Firebase Cloud Messaging, “in which the exploitation of FCM Server keys, stored within APK files [an Android file format], enabled the broadcasting of push notification messages to anyone using a Firebase-based application.”²⁶³

229. As these examples show, no computer security system is perfect. Even the best systems have a failure rate, so it is important for data processors such as Google to collect data parsimoniously, to provide users with accurate disclosures, and to provide easily understood privacy controls. Such measures can mitigate the harm when an inevitable security breach occurs.

230. Given its size, Google (and its users) are especially at risk. As noted above, Google has twenty-three data centers around the world, but does not publicly disclose its exact search volume or the total amount of data it stores—either cloud-stored data belonging to its users, or data about its users obtained through their web and app activity. It has been reported that Apple alone stores eight million terabytes of data on Google’s servers.²⁶⁴ The absence of statistics from Google notwithstanding, it is nonetheless safe to say that Google’s size renders it a tempting target for malicious actors.

8.3. Google Has a History of Privacy and Consent Failures

231. In 2010, Google admitted that Google Street View cars had been engaged not only in photography and cartography, but in collection of data—including personal online activity—from home wireless networks. Speaking as if the company were a white-hat hacker, Google representatives asserted that its faux pas illustrated the vulnerability of information stored on private networks.²⁶⁵

232. In 2012, researchers from Stanford University discovered that Google had intentionally circumvented the Safari browser’s default third-party cookie blocker, thereby negating the choice

²⁶² Antoinette Siu, “TikTok can circumvent Apple and Google privacy protections and access full user data, 2 studies say (Exclusive),” *Yahoo! News*, <https://www.yahoo.com/entertainment/tiktok-circumvent-apple-google-privacy-140000271.html> (February 14, 2022).

²⁶³ ITC Secure, “Firebase Cloud Messaging Vulnerability Potentially Affecting Billions,” <https://itcsecure.com/threat-horizon/firebase-cloud-messaging-vulnerability-potentially-affecting-billions/> (August 28, 2020).

ITC Secure, “Firebase Cloud Messaging vulnerability potentially affecting billions,” *ITC Secure*, <https://itcsecure.com/threat-horizon/firebase-cloud-messaging-vulnerability-potentially-affecting-billions> (August 28, 2020).

²⁶⁴ Joe Rossignol, “Apple reportedly storing over 8 million terabytes of iCloud data on Google servers,” *MacRumors*, <https://www.macrumors.com/2021/06/29/icloud-data-stored-on-google-cloud-increasing> (June 29, 2021).

²⁶⁵ Jemima Kiss, “Google admits collecting Wi-Fi data through Street View cars,” *The Guardian*, <https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data> (May 15, 2010).

Rodriguez v. Google

of Safari users not to have their online activity monitored—a practice that violated a prior FTC consent order. A new FTC investigation sparked by the discovery led to a \$22.5 million fine.²⁶⁶

233. In July 2017, the UK Information Commissioner ruled that the Royal Free Hospital had failed to comply with the Data Protection Act during its transfer of personal data of 1.6 million patients to Google subsidiary DeepMind for the development of Streams, an app intended to detect kidney injury. Although DeepMind was not held formally responsible for the violation, representatives acknowledged that their entire focus had been on “building tools that nurses and doctors wanted,” with little consideration for accountability “to patients, the public and the NHS as a whole.”²⁶⁷ The Streams app was adopted by numerous NHS trusts, but its use was eventually discontinued by all but the Royal Free Hospital, and the project was halted altogether in August 2021.²⁶⁸

234. Google has demonstrated that it cannot be trusted to disclose in a timely manner its own failure to protect users’ privacy. After discovering the aforementioned 2018 Google+ breach, Google disabled the insecure feature but chose not to notify users for fear of damaging the company’s reputation and attracting the scrutiny of government regulators. It also did not contact any of the 400+ application developers that had access to this non-public data to determine whether they had made use of it.²⁶⁹

235. After the October 2018 discovery, Google decided to shut down Google+ by August 2019. However, two months later, the company disclosed a second bug that had permitted the profile information of 52.5 million users—even from profiles set to “private”—to be exposed to outside developers via one of Google’s APIs.²⁷⁰

236. A 2018 Associated Press investigation found that many Google services on Android devices and iPhones continuously store location data regardless of user privacy settings that disallow it. Although Google responded to the findings by asserting that users have control over location settings in all the various tools that use them, users without a technical education cannot be expected to recognize that the “Turn Off Location History” option only affects a subset of applications, and that their location history continues to be collected and used by other

²⁶⁶ US Federal Trade Commission, “Google will pay \$22.5 million to settle FTC charges it misrepresented privacy assurances to users of Apple’s Safari internet browser,” <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> (August 9, 2012).

²⁶⁷ Alex Hern, “Royal Free breached UK data law in 1.6m patient deal with Google’s DeepMind,” *The Guardian*, <https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act> (July 3, 2017).

²⁶⁸ Natasha Lomas, “Google confirms it’s pulling the plug on Streams, its UK clinician support app,” *Tech Crunch*, <https://techcrunch.com/2021/08/26/google-confirms-its-pulling-the-plug-on-streams-its-uk-clinician-support-app> (August 26, 2021).

²⁶⁹ Douglas MacMillan and Robert McMillan, “Google exposed user data, feared repercussions of disclosing to public,” *Wall Street Journal*, <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194> (October 8, 2018).

²⁷⁰ David Thacker, “Expediting changes to Google+,” *The Keyword*, Google, <https://www.blog.google/technology/safety-security/expediting-changes-google-plus> (December 10, 2018).

Jillian D’Onofro, “Google is shutting down its Plus social network sooner than expected after discovering a second security bug,” *CNBC*, <https://www.cnn.com/2018/12/10/google-shutting-down-social-network-sooner-because-of-new-security-bug.html> (December 10, 2018).

Rodriguez v. Google

applications if the WAA setting is turned on. In some cases, detailed descriptions of Google’s use of Location History were only displayed to users in popups that appeared when users paused collection of Location History or reactivated the WAA setting.²⁷¹

237. Three days after publication of the Associated Press exposé on the persistence of Google location tracking, the company revised its help page for Location History settings, removing “With Location History off, the places you go are no longer stored” and adding “This setting does not affect other location services on your device” and “Some location data may be saved as part of your activity on other services, like Search and Maps.”²⁷²

238. In September 2019, Google and its subsidiary YouTube entered into a settlement with the FTC over allegations that the companies had illegally collected personal information from children—including cookies used to track their browsing—and served them with behaviorally targeted advertising without their parents’ consent. Fines totaling \$170 million were assessed, the largest penalty ever levied under the Children’s Online Privacy Protection Act since its inception.²⁷³

239. In February 2019, users of Google’s Nest security devices were shocked to learn that they contained an undisclosed microphone. Although purportedly included in order to detect intrusions, breaking glass, and the like, the microphones, whether inadvertently or deliberately activated, could also record and play back private conversations and the sounds of sexual activity.²⁷⁴

240. In mid-2019, an investigation by Dutch broadcaster VRT found that Google Home “smart speakers” were recording audio in users’ homes even when the speakers weren’t deliberately activated, and were passing those recordings along to contractors tasked with helping to improve the company’s speech recognition technology. When called to account for this invasion of customers’ privacy, Google representatives replied that users could simply turn the microphone off, even though they were required to opt in to voice recording in order to access Google Home features.²⁷⁵

241. In November 2019, the *Wall Street Journal* published an investigative report on Google’s theretofore-secret “Project Nightingale,” in which the company sought access to the healthcare data of millions of Americans in twenty-one states—data that included patient names and dates

²⁷¹ Ryan Nakashima, “Google tracks your movements, like it or not,” Associated Press, <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb> (August 13, 2018).

²⁷² Ryan Nakashima, “Google clarifies location-tracking policy,” Associated Press, <https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211> (August 16, 2018).

²⁷³ US Federal Trade Commission, “Google and YouTube will pay record \$170 million for alleged violations of children’s privacy law,” <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> (September 4, 2019).

²⁷⁴ Nick Bastone, “Google says the built-in microphone it never told Nest users about was ‘never supposed to be a secret’,” *Business Insider*, <https://www.businessinsider.com/nest-microphone-was-never-supposed-to-be-a-secret-2019-2> (February 19, 2019).

²⁷⁵ Joshua Bote, “Google workers are eavesdropping on your private conversations via its smart speakers,” *USA Today*, <https://www.usatoday.com/story/tech/2019/07/11/google-home-smart-speakers-employees-listen-conversations/1702205001> (July 11, 2019).

Rodriguez v. Google

of birth, lab results, diagnoses, and medication and hospitalization records, comprising an entire personal health record. The project began as a collaboration with the Ascension hospital chain, but neither doctors nor patients were informed of it, and were therefore unaware of the fact that non-anonymized medical records were available for review by Google staffers.²⁷⁶

242. In 2021, Google entered into an agreement with Nashville-based HCA Healthcare to consolidate and store patients' medical records and data from their medical devices. Dr. Michelle Mello, an adviser to Alphabet subsidiary Verily Life Sciences, acknowledged that records purportedly stripped of identifying information could nonetheless be combined with other data in a manner that enabled patients to be personally identified.²⁷⁷

243. In response to news of the Google-HCA deal, medical ethicist Dr. Arthur Kaplan expressed deep concern about the appropriateness of giving Google access to personal medical records, and called for updating US laws to strengthen privacy protection and mandate informed consent from patients whose records are accessed.²⁷⁸

244. Simultaneously with these announcements, Google launched a trial of a new feature, Federated Learning of Cohorts (FLoC), intended to replace third-party cookies. FLoC algorithmically sorted users into interest-based groups, based on their browsing history, for purposes of ad targeting. With the implementation of FLoC, it was planned that rather than allowing third parties to track Chrome users, Chrome would do the tracking.²⁷⁹ Shortly thereafter, security researcher Lukasz Olejnik discovered a flaw in FLoC whereby information was conveyed to websites about whether or not a user was employing Incognito mode.²⁸⁰ Up to

²⁷⁶ Rob Copeland, "Google's 'Project Nightingale' gathers personal health data on millions of Americans," *Wall Street Journal*, <https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790> (November 11, 2019).

Rob Copeland and Sarah E. Needleman, "Google's 'Project Nightingale' triggers federal inquiry," *Wall Street Journal*, <https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867> (November 13, 2019).

Rob Copeland, Dana Mattioli and Melanie Evans, "Inside Google's quest for millions of medical records," *Wall Street Journal*, <https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700> (January 11, 2020).

²⁷⁷ Melanie Evans, "Google strikes deal with hospital chain to develop healthcare algorithms," *Wall Street Journal*, <https://www.wsj.com/articles/google-strikes-deal-with-hospital-chain-to-develop-healthcare-algorithms-11622030401> (May 26, 2021).

²⁷⁸ Emily DeCiccio, "Privacy laws need updating after Google deal with HCA Healthcare, medical ethics professor says," CNBC, <https://www.cnbc.com/2021/05/26/privacy-laws-need-updating-after-google-deal-with-hca-healthcare-medical-ethics-professor-says.html> (May 26, 2021).

²⁷⁹ Gilad Edelman, "Google and the age of privacy theater," *Wired*, <https://www.wired.com/story/google-floc-age-privacy-theater> (March 18, 2021).

²⁸⁰ Thomas Claburn, "Google's 'privacy-first' ad tech FLoC squawks when Chrome goes Incognito, says expert. Web giant disagrees," *The Register*, https://www.theregister.com/2021/03/15/google_floc_chrome_incognito (March 15, 2021).

Rodriguez v. Google

5% of Chrome users were enrolled in FLoC's origin trial without Google having sought or received their consent.²⁸¹

245. In January 2022, Google announced that it was abandoning plans to institute FLoC in favor of a new advertising system called Topics, in which human curators (rather than algorithms) would sort users into interest groups based on their browsing history.²⁸² Chrome 94, introduced in September 2021, was the first version to enable "idle detection"—that is, developer queries regarding periods of device inactivity, which could be used to ascertain users' physical behavior, such as mealtimes and break times.²⁸³ Chrome 99, released in March 2022, still has this feature.

246. Google's internal documents indicate a lack of commitment on the part of upper management to maximizing user privacy. In a May 2020 planning document, senior research manager Arne de Booi observed that "Some current data practices and settings were not designed for the level of prominent explanation/consent regulators expect."²⁸⁴ Interviews conducted in October 2020 with members of Google's PrivacyNative team revealed concerns about Google management's commitment to user privacy in the company's increasingly complex universe of products. When asked, "What is the [Privacy and Data Protection Office's] current state? And privacy at Google?" Jonathan McPhie, Director of Product Management, replied, "There is no coherent strategy.... We don't have an articulated vision of how everything comes together."²⁸⁵ Google's Android and mobile privacy lead Giles Hogben stated, "We will not succeed at getting ourselves out of the hole unless we have privacy people in the C-Suite.... We need [a Senior Vice President] who is a privacy person. Not just a 10% part-time job that they have no experience in at all."²⁸⁶ Google product manager David Monsees agreed: "To enact change you need a politician to push this."²⁸⁷ Google Business Operations and Strategy Principal Yooki Park observed, "It is not that we are simple and the user doesn't get it. We are complex under the hood and on the surface. Our data infrastructure is not designed for privacy. There are

²⁸¹ Bennett Cyphers, "Google is testing its controversial new ad targeting tech in millions of browsers. Here's what we know," Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2021/03/google-testing-its-controversial-new-ad-targeting-tech-millions-browsers-heres> (March 30, 2021).

Zak Doffman, "Google's latest tracking nightmare for Chrome comes in two parts," *Forbes*, <https://www.Forbes.com/sites/zakdoffman/2021/10/02/stop-using-google-chrome-on-windows-10-android-and-apple-iphones-ipads-and-macs/?sh=4fcde6092f30> (October 2, 2021).

²⁸² Daisuke Wakabayashi, Kate Conger and Brian X. Chen, "Google introduces a new system for tracking Chrome browser users," *New York Times*, <https://www.nytimes.com/2022/01/25/business/google-topics-chrome-tracking.html> (January 25, 2022).

²⁸³ Dave LeClair, "Mozilla says Chrome's latest feature enables surveillance," *How-To Geek*, <https://www.howtogeek.com/756338/mozilla-says-chromes-latest-feature-enables-surveillance> (September 21, 2021).

²⁸⁴ GOOG-RDGZ-00090067 at -71

²⁸⁵ GOOG-RDGZ-00188868 at -77.

²⁸⁶ GOOG-RDGZ-00188868 at -80.

²⁸⁷ GOOG-RDGZ-00188868 at -85.

Rodriguez v. Google

core stakeholders at the company who think that it is impossible, or too hard to do and therefore not worth it.”²⁸⁸

247. Although Google employees and others involved in the web development, advertising, and software industries might assume that mechanisms of online tracking are a routine, ordinary part of life simply because they have become so prevalent and profitable, it is less likely that the general population would think that it is any more acceptable to be continuously, automatically tracked by unseen technologies than it would be to be tracked by flesh-and-blood parties.

248. All of these failures by Google to safeguard users’ information underscore the importance of offering users options in which Google does not collect, save, or use any information, and explains why users would desire and seek to take advantage of the promises that Google made about WAA and sWAA.

9. User Control over Google Tracking and Collection

9.1. Google Promises Users Control over the Company’s Collection of Their Data

249. Google has held itself out publicly as a champion of privacy, declaring that “what’s private is private, and the government should respect that”²⁸⁹—while at the same time profiting immensely from its collection of data on private citizens.

250. Google promises control. The first two sentences of the current Google Privacy Policy are: “When you use our services, you’re trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.”²⁹⁰ This promise to “put you in control” is part of Google’s efforts to assure people that they have control, including over Google’s collection, storage, and use of “your information.” The Privacy Policy also provides that “We will not reduce your rights under this Privacy Policy without your explicit consent.”

251. Google explicitly represents that the Web & App Activity setting allows users to control what Google collects. Since the May 25, 2018, Privacy Policy went into effect, Google has promised users that “across our services, you can adjust your privacy settings to control what we collect and how your information is used.” The Privacy Policy lists the “[p]rivacy controls” that Google offers to users, including “Activity Controls” such as “Web & App Activity.” The Privacy Policy directs users to “Go to Activity Controls” with a hyperlink, which leads to the Web & App Activity setting. Google has repeated these representations in every one of its eleven Privacy Policy versions since then.

252. A similar focus exists in Google’s “privacy and security principles,” where Google’s first principle states, “Respect our users. Respect their privacy.”²⁹¹ The principles describe how

²⁸⁸ GOOG-RDGZ-00188868 at -130.

²⁸⁹ Google, “Real surveillance reform: What’s private is private, and the government should respect that,” <https://www.google.com/takeaction/issue/surveillance> (first archived October 3, 2015).

²⁹⁰ Google, “Privacy policy,” <https://policies.google.com/privacy?hl=en-US> (December 15, 2022).

²⁹¹ Google, “Our privacy and security principles,” https://safety.google/principles/?hl=en_US (first archived June 5, 2020).

Rodriguez v. Google

people should be able to “access and review their data” and “delete it entirely” and “make it easy for people to control their privacy”—proclaiming that “privacy is always an individual choice that belongs to the user.”

253. In December 2018, Google CEO Sundar Pichai testified before Congress, asserting that Google clearly describes the extent of data that it collects. When asked by Chairman Bob Goodlatte, “Is it true that the Android operating system sends Google information every few minutes detailing the exact location of a smartphone within a few feet, the speed of movement of the phone, the altitude of the phone sufficient to determine what floor of the building the phone is on, the temperature surrounding the phone, and other readings, and if so, with Americans carrying their phones with them virtually at all times, doesn’t the collection of this volume of detailed information really mean that Google is compiling information virtually about every movement an individual with a smartphone is making every hour of every day?” Mr. Pichai did not deny the extent of data collection; rather, he dodged the question, stating that Google’s data collection is “a choice users make, we make it clear, and it depends on the use cases.”²⁹² Mr. Goodlatte interpreted Mr. Pichai’s answer as “yes,” this 24/7 collection does occur; Sam Heft-Luthy and Miguel Guevara, then product managers in Google’s Privacy and Data Protection Office (PDPO), interpreted it as “not great.”²⁹³

254. Mr. Pichai’s response reiterated the message of transparency and user control:

“For Google services, you have a choice of what information is collected, and we make it transparent.... In fact, in the last 28 days, 160 million users went to their My Account settings, where they can clearly see what information we have—we actually show it back to them. We give clear toggles, by category, where they can decide whether that information is collected, stored, or—more importantly—if they decide to stop using it, we work hard to make it possible for users to take their data with them.”²⁹⁴

“We are pretty explicit about data which we collect and give you protections for you to turn them on or off.”²⁹⁵

255. The clear import of Mr. Pichai’s testimony was that users could see *all* information Google is saving (“what information we have”), not that users lacked any transparency or control with respect to the full scope of Google’s collection, including when WAA or sWAA are off.

256. While it is true that Google Account holders may review and delete the data that Google saves to their “My Activity,” I have learned through my work in connection with this case that

²⁹² C-SPAN, “LIVE: Google CEO Sundar Pichai testifies on data collection (C-SPAN),” YouTube, <https://www.youtube.com/watch?v=WfbTbPEEJxI> at 43:10 (December 11, 2018).

²⁹³ GOOG-RDGZ-00087672, at -73.

²⁹⁴ C-SPAN, “LIVE: Google CEO Sundar Pichai testifies on data collection (C-SPAN),” YouTube, <https://www.youtube.com/watch?v=WfbTbPEEJxI> at 44:38 (December 11, 2018).

Sarah Perez, “Google’s CEO thinks Android users know how much their phones are tracking them,” *Tech Crunch*, <https://techcrunch.com/2018/12/11/google-ceo-sundar-pichai-thinks-android-users-know-how-much-their-phones-are-tracking-them> (December 11, 2018).

²⁹⁵ C-SPAN, “LIVE: Google CEO Sundar Pichai testifies on data collection (C-SPAN),” YouTube, <https://www.youtube.com/watch?v=WfbTbPEEJxI> at 3:33:31 (December 11, 2018).

Rodriguez v. Google

this is only the tip of the iceberg. Google simultaneously collects and saves a far broader range of user data, including data that Google saves while WAA and sWAA are off but that is never revealed to users through the settings referenced by Mr. Pichai.

257. Google’s efforts to feature “control” as one of the core principles for Google, both in its privacy policy and other public-facing documents, and in statements of its executives, falsely implies that Google collects and saves data only with user consent, and that users can stop Google’s collection, storage, and use of their data. In truth, turning off WAA and sWAA appears to give users even less control, placing Google’s collection, storage, and use of data generated by those users’ activity beyond any of the otherwise available controls.

258. Google has repeatedly touted its efforts to make its records of individual users’ activity available to them and subject to their control. The “My Activity” page displays a user’s search history, browsing history, and app usage history, including history of videos watched on YouTube.²⁹⁶ The “Takeout” page enables signed-in users to download a file containing emails, ad clicks, location, uploaded documents, and physical activity data.²⁹⁷ The implication is that this data is all the data that Google possesses for that user. As discussed below, that is false.

9.2. Giving Users Privacy Control Is Important for Google’s Brand, and Getting/Keeping Users

259. For years, Google scanned Gmail users’ emails to serve targeted advertising, but in June 2017, the company announced that it would end the practice—reportedly not so much out of concern for individual user privacy, but out of its desire to win the confidence and business of its largest customers.²⁹⁸

260. All of Google’s privacy promises are a key part of the Google brand. Google’s SEC filings recognize that Google’s “business depends on strong brands, and failing to maintain and enhance our brands would hurt our ability to expand our base of users, advertisers, customers, content providers, and other partners.”²⁹⁹

261. Google employees recognize both the personal and professional importance of privacy. For example, when asked if he “agree[d] that privacy is important,” Eric Miraglia, Senior Director of Product Management and the founder of Google’s Privacy and Data Protection Office, stated “I do” and added that “privacy is important [...] as a personal matter, as a matter of law. There’s lots of dimensions that it’s important.”³⁰⁰ Sam Heft-Luthy, a former Google product manager who was responsible for the “revamp” of Google’s Privacy Policy in 2018, similarly testified that “privacy is important to [him]” and that “a variety of users that we talk to from

²⁹⁶ Google, “My activity,” <https://myactivity.google.com> (first archived June 28, 2016).

²⁹⁷ Google, “Takeout,” <https://takeout.google.com> (accessed February 20, 2023).

²⁹⁸ Daisuke Wakabayashi, “Google will no longer scan Gmail for ad targeting,” *New York Times*, <https://www.nytimes.com/2017/06/23/technology/gmail-ads.html> (June 23, 2017).

²⁹⁹ Alphabet, “Form 10-K,” US Securities and Exchange Commission, <https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm> (December 31, 2020).

³⁰⁰ Miraglia Tr. 40:10-12, 41:4-6.

Rodriguez v. Google

different research initiatives ... would agree with that as well.”³⁰¹ He continued, explaining that “[g]iven that Internet technology is a major part of people’s lives, I think it’s important to have positive privacy experiences as people use the internet.”³⁰²

262. In surveys that Google has conducted, users have consistently responded that privacy and security are more important to them than anything else, and far more important than offering “high quality” or “user friendly” products and services.³⁰³ Google has strong business incentives to promote itself as a trustworthy guardian of privacy in order to sustain the user base that attracts advertisers to its platforms. This includes incentives for Google to continue offering and marketing its privacy “controls” and “settings,” notwithstanding any misconceptions or misunderstanding by users.

263. In fact, Google’s privacy efforts are primarily directed at building user trust in Google rather than delivering real protection. This was pointedly summarized in an October 2020 email to Google’s Privacy Surfaces team by Sam Heft-Luthy, who described building “[u]ser trust and affect—giving users a *sense* of the system as working to their benefit” as a “higher-level goal” that was “important but gameable without actually improving any of the underlying conditions.”³⁰⁴ [*emphasis in original*] Google prioritized the “gameable” goal of increasing users’ positive feelings towards Google over other measures of success, such as putting users “in a position of self-determination w.r.t. how their data is shared.”³⁰⁵

264. Across its numerous webpages and device screens, Google reassures users that they have control over the data Google collects. In the very first section of the Google Privacy Policy that took effect on May 25, 2018, for example, Google promised users that “across our services, you can adjust your privacy settings to control what we collect and how your information is used.”³⁰⁶ The Privacy Policy makes clear that among these “privacy controls” are Google’s “Activity Controls,” which include the Web & App Activity setting.

265. But the truth is that not even Google employees understand how—or whether—users can control the data Google collects. Mr. Heft-Luthy has testified that he had “incomplete knowledge of Google’s systems” during his time with the company, and that he was unable to recall “any specific piece of information that Google would not collect as a result of a user turning off the Web & App Activity control.”³⁰⁷ And in his February 2023 deposition, Google software engineer Xinyu Ye testified that he did not know what the Web & App Activity controls do, he did not know whether Google writes WAA-off data to any data source, and he did not know

³⁰¹ Heft-Luthy Rough Tr. 12:6-9.

³⁰² Heft-Luthy Rough Tr. 12:13-16.

³⁰³ GOOG-RDGZ-00014421, at -484.

³⁰⁴ GOOG-RDGZ-00173562.

³⁰⁵ GOOG-RDGZ-00173562.

³⁰⁶ GOOG-RDGZ-00000529.

³⁰⁷ Heft-Luthy Rough Tr. 53:4-10.

Rodriguez v. Google

whether Google uses WAA-off third-party data to refine Google Search or any other Google products.³⁰⁸

266. Google PDPO founder Eric Miraglia has testified that it's "important" to give users "control," which he interpreted as "choices about how data is collected and used."³⁰⁹ Mr. Miraglia went on to note, "there should be a regime of settings that are intelligible to users that allow them to control the way their data is collected and used and give them transparency over what's going on. We work really hard to provide that."³¹⁰ Yet, in a July 2019 email, Google's Security/Trust/Privacy manager Chris Ruemmler noted that "the activity controls wording...is very deceptive... I for one didn't realize Google actually stored all of my activity even if those controls were off and I work at Google! Seems sort of silly to turn them off as I'm not any safer with them off than on."³¹¹

267. Google's public relations on the subject notwithstanding, staffers have noted that privacy is not the company's strongest asset. In a series of interviews conducted in the summer and fall of 2020, numerous Google staffers offered their frank opinions on the state of privacy at Google.

- Google Android Director of Privacy Engineering Giles Hogben: "What I've observed is that Apple starts their design process from the marketing assertions they make—We want to be able to say 'what happens on your device stays on your device,' then they design around that statement—whereas we kind of build for usability and delight, then we think about the marketing statements later."³¹²
- Google Director of Product Management Guemmy Kim: "From a product and messaging perspective, we inundate users with proof points and controls, many products, and then users are like, what does this all mean? ...From a product perspective there is no product that is the point. Fundamentally we have to decide what our point is. There are too many competing messages which means that nothing lands and nothing resonates with the users.... What is the concept the user understands? ...what is sWAA vs WAA vs YT? They don't make sense because of the naming and there are hidden functions that people don't know. Like Chrome sync and others that I don't even understand and can't describe.... There is no central way that everyone across products are handling privacy."³¹³
- Google Director of Engineering for Privacy and Security Stephan Micklitz: "We need to have to have the infrastructure in place to understand how we use user data—which we don't do (completely) today.... The way we have set up the system has amounted to a mountain of complexity which makes it hard for us to move quickly. Because everything is distributed and nobody knows how everything works we need to talk to a lot of people to make changes."³¹⁴

³⁰⁸ Ye Rough Tr. 13:11-20; 16:3-9; 22:4-7.

³⁰⁹ Miraglia Tr. 41:23-42:3.

³¹⁰ Miraglia Tr. 97:13-17.

³¹¹ GOOG-RDGZ-00024709 at -09.

³¹² GOOG-RDGZ-00188868 at -81.

³¹³ GOOG-RDGZ-00188868 at -92, 97, 93, 94.

³¹⁴ GOOG-RDGZ-00188868 at -96

Rodriguez v. Google

- Google software engineer Bryan Horling: “I am not sure that our strategies are the right ones right now.... Some of our previously well-intentioned directions where products want to get people into a good state doesn’t necessarily serve our users well. A strategy focusing on conservative defaults might be better. But this is a bitter pill to swallow—products do less by default.”³¹⁵
- Google principal engineer Othar Hansson: “We assume the user would trust us and we would get all the data in the account with one privacy policy. It turned out that this doesn’t work and with GDPR it is not acceptable even. At Google we still seem to believe in that fantasy that users agreed to this.... One example are all the controls we have that have horrible names and don’t mean anything to anyone, not even within the company.... We don’t have clear principles, we don’t give teams clear advice.... The way we do engineering at Google is by assuming that we control everything and that nothing will change.”³¹⁶

9.3. Google’s Notice and Consent Procedures Are Confusing

268. In *The New Digital Age*, Eric Schmidt and Jared Cohen stated that, “People have a responsibility as consumers and individuals to read a company’s policies and positions on privacy and security before they willingly share information,” and shortly thereafter predicted that technology companies will “also have to hire more lawyers.”³¹⁷

269. To test the validity of Schmidt and Cohen’s concept of Google users’ responsibility to read—and presumably understand—Google’s policies, I input the texts of two Google policies into an online readability calculator.³¹⁸ (Readability calculators are a common tool to test the readability of documentation, and have been used by Google to analyze proposed disclosures.³¹⁹)

270. This readability calculator applies several readability measures—that is, mathematical formulae—that are commonly used to evaluate the comprehensibility of technical documentation, medical writing and other complex public communications. The Coleman-Liau Index,³²⁰ Flesch Kincaid Grade Level,³²¹ Automated Readability Index,³²² SMOG (Simple

³¹⁵ GOOG-RDGZ-00188868 at -99.

³¹⁶ GOOG-RDGZ-00188868 at -915-916.

³¹⁷ Eric Schmidt and Jared Cohen, *The New Digital Age*, Knopf, https://archive.org/details/newdigitalageres0000schm_w0t9 (2013), pp. 65, 66.

³¹⁸ https://www.online-utility.org/english/readability_test_and_improve.jsp

³¹⁹ GOOG-RDGZ-00090067 at -82.

³²⁰ Wikipedia, “Coleman-Liau index,” https://en.wikipedia.org/wiki/Coleman%E2%80%93Liau_index (accessed February 20, 2023).

³²¹ Wikipedia, “Flesch-Kincaid readability tests,” https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests (accessed February 20, 2023).

³²² Wikipedia, “Automated readability index,” https://en.wikipedia.org/wiki/Automated_readability_index (accessed February 20, 2023).

Rodriguez v. Google

Measure of Gobbledygook),³²³ and Gunning-Fog Index,³²⁴ estimate the US grade level required to comprehend a text; the Flesch Reading Ease uses a scale of 1–100.³²⁵ “Lexical density” is a measure of the structure and complexity of a text.³²⁶

271. Google’s April 14, 2014, Terms of Service and June 28, 2016, Privacy Policy are the policies in force at the beginning of the class period, which I understand began on July 1, 2016, and is ongoing. Their readability results:

Google Terms of Service (April 14, 2014)	
Number of characters (without spaces)	9,347.00
Number of words	1,920.00
Number of sentences	99.00
Lexical Density	49.90
Average number of characters per word	4.87
Average number of syllables per word	1.71
Average number of words per sentence	19.39
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	12.24
<i>Approximate representation of the US grade level needed to comprehend the text</i>	
Coleman Liau index	11.33
Flesch Kincaid Grade level	12.14
ARI (Automated Readability Index)	11.20
SMOG	13.56
<i>Scale of 1–100, with lower scores more difficult to read and higher scores easier to read</i>	
Flesch Reading Ease	42.54

Google Privacy Policy (June 28, 2016)	
Number of characters (without spaces)	20,613
Number of words	4,064
Number of sentences	194
Lexical Density	53.47
Average number of characters per word	5.07
Average number of syllables per word	1.76
Average number of words per sentence	20.95
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	

³²³ Wikipedia, “SMOG,” <https://en.wikipedia.org/wiki/SMOG> (accessed February 20, 2023).

³²⁴ Wikipedia, “Gunning fog index,” https://en.wikipedia.org/wiki/Gunning_fog_index (accessed February 20, 2023).

³²⁵ Wikipedia, “Flesch-Kincaid readability tests,” https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests (accessed February 20, 2023).

³²⁶ Wikipedia, “Lexical density,” https://en.wikipedia.org/wiki/Lexical_density (accessed February 20, 2023).

Rodriguez v. Google

Gunning Fog index	14.02
<i>Approximate representation of the US grade level needed to comprehend the text</i>	
Coleman Liau index	12.64
Flesch Kincaid Grade level	13.33
ARI (Automated Readability Index)	12.93
SMOG	13.89
<i>Scale of 1–100, with lower scores more difficult to read and higher scores easier to read</i>	
Flesch Reading Ease	36.79

272. In short, the documents that form the backbone of Google’s notification to Google Account holders of its privacy policies are long, dense, and hard to read, and things haven’t gotten much better over time. (Appendix 3 to this report contains the results of readability tests for all of the versions of these two Google policies from the beginning of the class period through December 15, 2022, and information on the various formulae used.) The Privacy Policy, in particular, requires the user to have at least some college education to easily understand on the first reading.

273. According to the Pew Research Center, in 2021, 93% of adults in the United States use the Internet, including 86% of high school graduates or adults without a high school diploma.³²⁷ Presumably, a great many of these adults use Google services, including the Google Chrome browser, the Google Chrome search and browser apps, Android smartphones, and smartphone apps that use Google services.

274. From the beginning of the class period to December 15, 2022, Google has issued a total of twenty-three versions of these documents:

- Terms of Service: Four versions between April 14, 2014, and January 25, 2022 (total 11,335 words); and
- Privacy Policy: Nineteen versions between June 28, 2016, and December 15, 2022 (total 127,488 words).

275. The total word count of all of the versions of these documents in force during the class period exceeds 138,000 words, which translates to over 276 pages of single-spaced text or 552 pages of double-spaced text, with an estimated reading time of nearly 460 minutes—that is, nearly eight hours.³²⁸ Of course, this estimated reading time assumes that the reader is capable of comprehending the text, which in many cases is unlikely.

276. The time span between revisions of these policies has at times been quite short, with as many as four revisions issued in the space of a year. Take, for example, revisions of the Privacy Policy:

³²⁷ Pew Research Center, “Internet/broadband fact sheet,” <https://www.pewresearch.org/internet/fact-sheet/internet-broadband> (April 7, 2021).

³²⁸ Capitalize My Title, “How many pages is 138,000 words?” <https://capitalizemytitle.com/page-count/138000-words> (accessed February 10, 2023).

Rodriguez v. Google

- Revised June 28, 2016, then again eight weeks later, on August 29, 2016;
- Revised March 1, 2017, then about six weeks later on April 17, 2017;
- Revised October 15, 2019, then eight weeks later on December 19, 2019;
- Revised July 1, 2020, then eight weeks later on August 28, 2020, then four weeks later on September 30, 2020.

277. The many versions of these documents notwithstanding, their readability has not improved over time; in fact, over the course of the class period, the readability scores of the Terms of Service and Privacy Policy have deteriorated:

- The April 14, 2014, Google Terms of Service had a Flesch Reading Ease score of 42.54—that is, difficult to read. This particular score dropped with each successive version, with the January 25, 2022, version weighing in at 31.21—that is, very difficult to read.
- The June 28, 2016, Google Privacy Policy has a Flesch Reading Ease score of 36.79—that is, difficult to read; the December 15, 2022, version has a score of 28.60—that is, very difficult to read.

278. Each of these Google policy documents contains numerous links to other pages on Google’s website, which direct users to notices pertaining to specific features, such as the WAA Help Page. Additional explanatory text is also hidden in 100 tooltip links sprinkled throughout the current version of the Privacy Policy.

9.4. Google Uses Dark Patterns

279. As previously defined in Section 6.3, dark patterns are user interface designs that serve to manipulate users into making choices that are contrary to their own interests. In terms of discussing the WAA and sWAA settings, it is helpful to consider the context of the broader range of controls and complexity presented by Google.

280. A 2018 study by the Norwegian Consumer Council found that Google frequently employed default settings that were preselected to the least privacy-friendly options.³²⁹ Settings were often hidden or obscured so that they would never be seen by users who reflexively click the “Agree” button without exploring their options. To read the full text of Google’s GDPR popup required testers to scroll through screens of text.

281. At Privacy Dashboard, authorizing personal data collection for the purpose of ad personalization was described as “Make ads more relevant to you”; in contrast, testers who attempted to disable personal data collection were confronted with warnings that “You’ll still see ads, but they’ll be less useful to you.” Data collection was characterized as a positive option; opting out was met with warnings that functionality of Google products and Android apps might be compromised. “Nudging” tactics included warnings that disabling ad personalization might also disable users’ ability to “mute” ads, which could lead some users to fear that video

³²⁹ Forbrukerrådet (Norwegian Consumer Council), “Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy,” <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> (June 27, 2018).

Rodriguez v. Google

advertisements might blare away at their workplace if they didn't click "Agree"—an understandable fear given the commonly understood definition of "mute" as "to deaden, soften, or muffle the sound of (a person or thing)."³³⁰ Google failed to explain in context its idiosyncratic definition of "mute" as the ability to control ads that they see—a definition that has nothing to do with volume or whether or not users saw ads in the first place. Testers had to navigate to a separate page to learn that.³³¹

282. Google trumpets users' ability to "take control of their data," and claims that they may "easily delete specific items or entire topics." However, the Norwegian Consumer Council's Privacy Dashboard testers navigated through thirty to forty different links in their search for the "delete all location data" option. The vaguely titled "My Activity" page allowed bulk deletion of data. The testers found that separate controls were required to manage Google Maps data and Google Location History. They were unable to locate any option to delete the entire location history, only individual points, and found that deleting Google Maps data did not delete their Location History. To do that, they resorted to Google search, which yielded a link to the company's support site; an additional tester discovered that the option to delete the entire Location History was linked only from a small image of a trashcan.

283. In sum, the Norwegian investigators found that "by giving users an overwhelming amount of granular choices to micromanage, Google has designed a privacy dashboard that, according to our analysis, actually discourages users from changing or taking control of the settings or delete bulks of data."³³²

284. The conclusions of the Norwegian Consumer Council are echoed in at least two presentations to Google's CEO by Google employees. In an August 2019 presentation to Sundar Pichai, Senior Interaction Designer Max Walker noted that Chrome's "privacy-related controls are hidden in the advanced section of settings and on subpages. They are overwhelming and difficult to understand."³³³ This point was reiterated in another presentation to Pichai, made in September 2019, in which members of Google's Chrome Trust and Safety team warned that Chrome's third-party cookie blocking controls were "too hard to find and understand."³³⁴

285. This is by no means the only investigation of dark patterns by Google. Harry Brignull, the cognitive scientist who coined the term "dark patterns," collects examples of dark patterns in Internet design. The "Hall of Shame" on his website lists over 400 examples, with Google as one of the four most commonly complained-about companies.³³⁵

³³⁰ *Oxford English Dictionary Online*, "Mute" (retrieved March 7, 2022).

³³¹ Google, "Mute ads on sites that partner with Google," <https://support.google.com/authorizedbuyers/answer/2695260?hl=en> (accessed February 20, 2023).

³³² Forbrukerrådet (Norwegian Consumer Council), "Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy," <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> (June 27, 2018).

³³³ GOOG-RDGZ-00206996 at -7004.

³³⁴ GOOG-RDGZ-00184248 at -68.

³³⁵ Harry Brignull, "Hall of shame," *Deceptive Design*, <https://www.deceptive.design/hall-of-shame/all> (accessed December 20, 2022).

Rodriguez v. Google

286. Designer Johnny Makes has described how changes in the design of the Google Search results page result in increased density of advertisements, and less distinction between ads and organic search results: “Over the years, Google have been repeatedly reducing the strength of any visual indicators that gave away adverts; first removing the helpful background colour, then switching to a small (but at least solid) coloured icon, that too finally giving way to a thin coloured outline. The most recent iteration alters the (legally required) advert indicator to plain black text, and ramps up the noise on all other search results, burying the advert ‘signal’ to users.”³³⁶

287. In 2014, the FTC settled with Google over its use of dark patterns that resulted in parents being unwittingly billed for in-app purchases made by their children. “According to the complaint, in mid- to late 2012, Google began presenting a pop-up box that asked for the account holder’s password before billing in-app charges. The new pop-up, however, did not contain any information about the charge. Google also did not inform consumers that entering the password opened up a 30-minute window in which a password was no longer required, allowing children to rack up unlimited charges during that time.”³³⁷ This was not identified as a dark pattern in 2014—the phrase was too new then—but was referenced in a 2022 FTC report on the topic.³³⁸

288. In their 2018 presentation to the Conference on Human Factors in Computing Systems, Colin Gray and colleagues described how Google users who turn off location services are shown a pop-up with a prompt encouraging them to enable it, even when apps are not running; the popup displays controls for “agree” and “disagree,” and a tiny “Don’t show again” checkbox. Whereas users who “agree” never see the popup again, those who disagree are repeatedly nagged to reinstate location services, even absent any impairment in the functioning of the apps they use.³³⁹

289. Google’s use of dark patterns has also been extensively investigated by France’s data protection agency, *Commission Nationale de l’Informatique et des Libertés* (CNIL). In January 2019, CNIL fined Google \$63.2 million, citing lack of transparency, insufficient information, and failure to obtain valid consent to data collection for the purpose of nonessential ad personalization during the initial configuration of Android mobile devices. CNIL found that Google’s privacy policy and terms of use, and the design of Google’s interface, did not enable users to readily identify all of the services, websites and apps that processed personal data, or

³³⁶ Johnny Makes, “Why Google’s new search results design is a dark pattern,” *UX Design*, <https://uxdesign.cc/why-google-new-search-results-design-is-a-dark-pattern-168935802f95> (January 23, 2020).

³³⁷ US Federal Trade Commission, “Google to refund consumers at least \$19 million to settle FTC complaint it unlawfully billed parents for children’s unauthorized in-app charges,” <https://www.ftc.gov/news-events/news/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it-unlawfully-billed-parents-childrens> (September 4, 2014).

³³⁸ US Federal Trade Commission, “Bringing dark patterns to light,” Staff Report, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (September 2022).

³³⁹ Colin M. Gray, et al., “The dark (patterns) side of UX design,” CHI 2018, Montreal, Quebec, Canada, <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (April 21-26, 2018).

Alison Hung, “Keeping consumers in the dark: Addressing ‘nagging’ concerns and injury,” *Columbia Law Review* 121, <https://columbialawreview.org/content/keeping-consumers-in-the-dark-addressing-nagging-concerns-and-injury> (2021).

Rodriguez v. Google

specify the uses to which that data would be put. Further, “there is an overall lack of accessibility to the information provided by the company in the context of the processing in question.” Users who did not wish to “Accept All” cookies could not reject cookies with a single click, but were directed to take another step, by clicking on a “More options” link. In short: through its user interface, Google encouraged users to easily accept tracking, but did not fully explain what it was they were being asked to accept, and made it more difficult to reject some or all cookies.³⁴⁰

290. In December 2020, CNIL fined Google again—this time it was \$120 million for placing tracking cookies on users’ computers and mobile devices without their consent. CNIL found that Google automatically placed cookies on the browsers and browser apps of visitors to <http://www.google.fr> before a consent screen was displayed, and that the screen did not disclose that the cookies had already been placed or describe their function. Regulators also discovered that if a user opted to deactivate personalized advertising, one cookie remained and continued to process data. The size of the fine was justified, they stated, by the widespread use of Google Search in France, by the impact of the company’s practices on nearly the entire French population, and by the sizeable profits Google derived from cookie-enabled advertising. Although Google discontinued on-load cookie placements in September 2020, CNIL found that a new cookie notice presented to arriving users still did not clearly describe the function of the tracking cookies, or adequately inform users that they could refuse them.³⁴¹ The fine was confirmed in January 2022.³⁴²

291. In a separate January 2022 action, France’s CNIL fined Google again (along with Google’s subsidiary YouTube, and Meta Platforms’ Facebook) for their continued use of “dark patterns” that “do not make refusing cookies as easy as to accept them.”³⁴³ The three companies, regulators observed, “offer a button allowing the user to immediately accept cookies. However, they do not provide an equivalent solution (button or other) enabling the Internet user to easily refuse the deposit of these cookies. Several clicks are required to refuse all cookies, against a

³⁴⁰ Commission Nationale de l’Informatique et des Libertés, “Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC,” <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> (January 21, 2019).

Lucie Audibert, “Beware ‘dark patterns’: Data protection regulators are watching,” TaylorWessing, <https://globaldatahub.taylorwessing.com/article/beware-dark-patterns-data-protection-regulators-are-watching> (March 2020).

³⁴¹ Natasha Lomas, “France fines Google \$120M and Amazon 42M for dropping tracking cookies without consent,” *Tech Crunch*, <https://techcrunch.com/2020/12/10/france-fines-google-120m-and-amazon-42m-for-dropping-tracking-cookies-without-consent> (December 10, 2020).

³⁴² Commission Nationale de l’Informatique et des Libertés, “Cookies: The Council of State confirms the sanction imposed by the CNIL in 2020 on Google LLC and Google Ireland Limited,” <https://www.cnil.fr/en/cookies-council-state-confirms-sanction-imposed-cnil-2020-google> (January 28, 2022).

³⁴³ Commission Nationale de l’Informatique et des Libertés, “Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation,” <https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance> (January 6, 2022).

Rodriguez v. Google

single one to accept them.” It was concluded that this practice violates users’ freedom of consent.³⁴⁴

292. In 2022, Gabriel Weinberg, CEO of search engine DuckDuckGo, alleged that Google deploys “manipulative design... to trick users into abandoning rival products.” These design tricks include pushing misleading notifications that badger users into disabling the DuckDuckGo browser extension; delaying installation of the extension until the user answers whether they still want to “Change back to Google Search”; and displaying the “Change back” option within a larger, more prominent button than the control to complete the installation.³⁴⁵

293. A 2022 FTC report describes another Google dark pattern: “the set-up flow for Google’s Android phones, which the researcher argued encourages consumers to enable location collection because ‘the way [Google] portrayed the choices was in such a manner that you would turn on location tracking.’”³⁴⁶

294. Users are not the only victims of Google’s dark patterns. A 2022 analysis describes a dark pattern in Firebase that is implemented at the expense of Google’s paying *customers*: namely, app developers and advertisers. Because Google offers no fixed-price plan, and because the mechanisms to limit overspending are inadequate, customers are regularly surprised by their bills.³⁴⁷

295. Other design tricks that serve to manipulate Google customers into paying more for its services involve Google Ads (formerly Adwords).³⁴⁸ By manipulating default settings and requiring the advertiser to do extra work to change them, Google nudges advertisers to select “broad match” for positive keywords—that is, search terms chosen to trigger the display of an advertisement—and “exact match” for negative keywords—that is, search terms chosen to block the display of an advertisement. Whereas with “broad match,” “ads may show on searches that include misspellings, synonyms, related searches and other relevant variations,” “exact match” means just that.³⁴⁹ By selecting “exact match” for negative keywords, fewer searches block the display of irrelevant ads, more ads are displayed, and customers’ monthly advertising bills go up. Google also preselects the “Include Google Display Network” option, which authorizes the

³⁴⁴ Scott Ikeda, “Google and Facebook hit with fines over dark patterns allegedly misleading users into cookie consent,” *CPO Magazine*, <https://www.cpomagazine.com/data-protection/google-and-facebook-hit-with-fines-over-dark-patterns-allegedly-misleading-users-into-cookie-consent> (January 11, 2022).

³⁴⁵ Cristiano Lima and Aaron Schaffer, “Google is manipulating browser extensions to stifle competitors, DuckDuckGo CEO says,” *Washington Post*, <https://www.washingtonpost.com/politics/2022/01/05/google-is-manipulating-browser-extensions-stifle-competitors-duckduckgo-ceo-says> (January 5, 2022).

³⁴⁶ US Federal Trade Commission, “Bringing dark patterns to light,” Staff Report, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (September 2022).

³⁴⁷ Minima, “Firebase billing surprises: How to really cap your spending,” <https://blog.minimacode.com/cap-firebase-spending> (January 28, 2022).

³⁴⁸ Dennis Moons, “Dark patterns in Google Ads,” *Store Growers*, <https://www.storegrowers.com/dark-patterns-google-ads> (December 12, 2022).

³⁴⁹ Google, “About keyword matching options,” *Search Ads 360 (new experience) Help*, <https://support.google.com/sa360/answer/9322510> (accessed January 13, 2023).

Rodriguez v. Google

display of ads not only on Google Search results pages that contain selected keywords, but also, indiscriminately, on third-party sites and mobile apps.

VI. Google Tracking and Web & App Activity Topics

10. WAA and User Control

10.1. Google Presented WAA and sWAA as Ways for Users to Control Their Privacy

296. As part of my analysis for this case, I reviewed Google’s representations during the class period concerning privacy, control, and the WAA and sWAA settings, including the different versions of Google’s Terms of Service, Google’s Privacy Policy, and various WAA- and sWAA-specific disclosures like the WAA Help Page (currently titled, “Find and control your Web & App Activity”).³⁵⁰ These were documents that Google made publicly available.

297. While these Google documents included some high-level disclosures relating to Google’s practices, none of them provided notice that Google would collect and save app-activity data even if the user switched off WAA and/or sWAA. To the contrary, throughout these documents, Google represented that users were in control of the data that Google collects, saves, and uses, and that users could exercise this control through “privacy settings” such as WAA and sWAA—free from Google’s surveillance.

298. Google’s Terms of Service throughout the class period expressly pointed users to Google’s Privacy Policy so that they could understand Google’s obligations with respect to collection, storage, and use of users’ data.³⁵¹ Google’s Terms of Service dated April 14, 2014, and October 25, 2017, both reiterated how “Google’s privacy policies explain how [Google] treat[s] your personal data and protect[s] your privacy when you use [Google’s] Services.” (The March 2020 version of the TOS purports to exclude the Privacy Policy.³⁵²) Google’s Terms of Service do not disclose Google’s collection of the app activity of logged-in Google account holders who had switched their WAA and/or sWAA controls to “off.”

299. Google’s Privacy Policy throughout the class period promised that users had control over Google’s collection of their information, with users able to exercise that control by using the Activity Controls settings, which include WAA and sWAA.³⁵³ From August 29, 2015, to May

³⁵⁰ Google, “Find & control your Web & App Activity,” <https://support.google.com/accounts/answer/54068?hl=en&co=GENIE.Platform%3DAndroid> (accessed December 20, 2022).

³⁵¹ GOOG-RDGZ-00000923 (effective April 14, 2014), GOOG-RDGZ-00000929 (effective October 25, 2017).

³⁵² GOOG-RDGZ-00000935 (effective March 31, 2020).

³⁵³ Google’s Second Supplemental Responses to Interrogatories 6-8 list various versions of the Google Privacy Policy by Bates number: GOOG-RDGZ-00000400 (effective August 19, 2015), GOOG-RDGZ-00000417 (effective March 25, 2016), GOOG-RDGZ-00000434 (effective June 28, 2016), GOOG-RDGZ-00000451 (effective August 29, 2016), GOOG-RDGZ-00000468 (effective March 1, 2017), GOOG-RDGZ-00000485 (effective April 17, 2017), GOOG-RDGZ-00000502 (effective October 2, 2017), GOOG-RDGZ-00000519 (effective December 18, 2017), GOOG-RDGZ-00000529 (effective May 25, 2018), GOOG-RDGZ-00000557 (effective January 22, 2019), GOOG-RDGZ-00000585 (effective October 15, 2019), GOOG-RDGZ-00000613 (effective December 19, 2019), GOOG-RDGZ-00000642 (effective March 31, 2020), GOOG-RDGZ-00000672 (effective July 1, 2020), GOOG-RDGZ-

Rodriguez v. Google

24, 2018, Google’s Privacy Policy represented that Google wanted to be “clear about what information [Google] collect[s].” In versions of the Privacy Policy in effect during this period, Google emphasized “transparency and choice,” and suggested users had “control” of “who [they] share information with.” Nowhere in these versions of the Privacy Policy did Google disclose its collection of the mobile app activity of logged-in Google account holders who had switched their WAA and/or sWAA controls to “off.”

300. Beginning with the May 25, 2018, version, Google’s Privacy Policy became even more categorical in emphasizing users’ control over collection of their data. As noted previously, the first two sentences on the first page of these versions of the Privacy Policy promise (in enlarged font):

When you use our services, you’re trusting us with your information. We understand this is a big responsibility and work hard to protect your information and ***put you in control.***³⁵⁴ (emphasis added)

301. The Privacy Policy from May 25, 2018, through February 9, 2022, also contained a section regarding “My Activity,” promising that “My Activity allows you to review and control data that’s created when you use Google services.” A hyperlink, “Go to My Activity,” brought users to a page where they could turn off WAA. The Privacy Policy has also since May 25, 2018, defined “Google services” to include “Products that are integrated into third-party apps and sites, like ads, analytics” (i.e., Google Analytics for Firebase, AdMob, and Ad Manager).

302. Beginning with Google’s February 10, 2022, Privacy Policy, Google changed its explanation of My Activity, representing that “My Activity allows you to review and control data that’s saved to your Google Account.” Google also added a description about sWAA: “control whether information about your activity on other sites, apps, and devices that use Google services, such as apps you install and use on Android, is saved in your Google Account and used to improve Google services.” That text includes a hyperlink that brings users to the WAA Help Page, discussed below.

303. In these newer Privacy Policies, Google does not inform users that Google collects and saves data from signed-in users that it stores outside of “My Activity.” To the contrary, Google informs users that “across our services, you can adjust your privacy settings to control what we collect and how your information is used,” and that these “[p]rivacy controls” include “Activity Controls,” including Web & App Activity.

00000703 (effective August 28, 2020), GOOG-RDGZ-00000735 (effective September 30, 2020), GOOG-RDGZ-00188616 (effective February 4, 2021), GOOG-RDGZ-00188632 (effective July 1, 2021), GOOG-RDGZ-00188602 (effective February 2, 2022). All but the August 19, 2015, February 4, 2021, July 1, 2021 and February 2, 2022 versions produced by Google consist of a single page, and are incomplete. I have therefore relied upon the versions archived online at <https://policies.google.com/privacy/archive>.

³⁵⁴ As noted above, all but four versions of the Privacy Policy produced by Google consist of a single page, and are incomplete. I have therefore relied upon the versions archived online at <https://policies.google.com/privacy/archive>, including versions dated October 4, 2022 and December 15, 2022, which were published after Google prepared its Second Supplemental Responses to Interrogatories, Set Three. Both of these newer versions contain the same promise of “control” discussed above.

Rodriguez v. Google

304. Google’s behavior is analogous to a hotel that promises there are no secret cameras in your room recording your activities on videotape, but when discovered, argues that their promise of “no videotape” is true, and that they only transmitted images to a remote, unknown location, where your data is preserved forever. The latter is even worse than the former. If the private data were stored locally, a user might be able to find and erase it.

10.2. Anonymization Does Not Protect the Privacy of WAA and sWAA Data

305. Google’s disclosures about WAA indicate that turning off WAA or sWAA will prevent Google from collecting, saving, and using their app activity. There are a number of reasons why users might wish to prevent this.

306. Users may seek to avoid being tracked in their use of apps that address health conditions (for example, the urinary incontinence tracker Bladder Diary), hoping that their activity will **not** be saved and thereby give off clues about an embarrassing medical concerns.³⁵⁵ Other very personal and potentially embarrassing medical topics include impotence, infertility, irritable bowel syndrome, birth control, abortion, mental illness, cancer, HIV status, COVID-19 status, and drug addiction.

307. Users may also seek to avoid being tracked in their use of apps related to job-hunting (e.g., LinkedIn, Indeed, Monster), messaging (e.g., Telegram, Signal), religion (e.g., Daily Islam, Book of Mormon), counseling (e.g., CBT Thought Diary, Suicide Safety Plan), finance (e.g., NerdWallet, Fidelity), probation (e.g., Case Connect Mobile), legal cannabis purchases (e.g., Leafly, Weedmaps), and nearly every other imaginable subject.

308. However, as I have discussed in Section 6.2, pseudonymization does not protect the privacy of data generated by users who have switched their WAA/sWAA controls to “off.” App users are sufficiently unique to allow “pseudonymized” app usage data to be correlated with other, identified, data, as Google employees readily admit.

309. This potential is not merely theoretical. Several companies sell software libraries that give developers the capability of uniquely identifying—that is, fingerprinting—app users, even if those users don’t want to be identified. One 2018 study found eight different fingerprinting libraries that were used in 19% of the 30,000 Android apps they checked.³⁵⁶

310. Another 2018 research paper looked specifically at Android web-to-app communications, and demonstrated that users of Android apps can be uniquely identified through a variety of different mechanisms, none of which require any extraordinary access.³⁵⁷ The authors were able to join disparate databases of user browsing data with their app usage data. They term their techniques “session fingerprinting,” since their goal is to identify web-browsing sessions and app

³⁵⁵ Caner Baran, and Safak Yilmaz Baran, “YouTube videos as an information source about urinary incontinence,” *Journal of Gynecology, Obstetrics and Human Reproduction* 50, no. 10, <https://www.sciencedirect.com/science/article/abs/pii/S2468784721001343?via%3Dihub> (December 2021).

³⁵⁶ Christof Ferreira Torres and Hugo Jonker, “Investigating fingerprinters and fingerprinting-alike behaviour of Android applications,” *European Symposium on Research in Computer Security (ESORICS 2018) Proceedings*, Springer-Verlag, https://link.springer.com/chapter/10.1007/978-3-319-98989-1_4 (August 7, 2018).

³⁵⁷ Efthimios Alepis and Constantinos Patsakis, “Session fingerprinting in Android via web-to-app intercommunication,” *Security and Communication Networks*, <https://dl.acm.org/doi/10.1155/2018/7352030> (2018).

Rodriguez v. Google

usage on the same device and identify the user. This means that a company like Google would be able to use its identified browsing information about users to identify WAA-off users.

11. Google's Use of Dark Patterns

11.1. Google's WAA Help Page Exemplifies Dark Patterns

311. In Colin Gray's taxonomy, "sneaking" is defined as "attempt[s] to hide, disguise, or delay the divulging of information that has relevance to the user. Sneaking often occurs in order to make the user perform an action they may object to if they had knowledge of it. Sneaking behaviors may include additional undisclosed costs or undesired effects from a particular action." Gray additionally defines "hidden information" as "options or actions relevant to the user but not made immediately or readily accessible."³⁵⁸

312. The FTC's category of "sneaking or information hiding" includes "tricking a shopper into buying unwanted items by using a pre-checked box" and "hiding material information or significant product limitations from people."³⁵⁹

313. The EU's category "left in the dark" includes "ambiguous wording or information," which results in users being "left unsure of how data will be processed or how to exercise control over their personal data."³⁶⁰

314. Google's WAA Help Page exemplifies these dark patterns. The page explains how WAA ostensibly gives users control over whether or not Google saves their data:

Find & control your Web & App Activity

If Web & App Activity is turned on, your searches and activity from other Google services are saved in your Google Account, so you may get more personalized experiences, like faster searches and more helpful app and content recommendations.

You can turn Web & App Activity off or delete past activity at any time.³⁶¹

³⁵⁸ Colin M. Gray, et al., "The dark (patterns) side of UX design," CHI 2018, Montreal, Quebec, Canada, <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (April 21-26, 2018).

³⁵⁹ US Federal Trade Commission, "Bringing dark patterns to light," Staff Report, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (September 2022).

³⁶⁰ Andrea Jelinek, et al., "Dark patterns in social media platform interfaces: How to recognise and avoid them," Version 1.0, European Data Protection Board, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (14 March 2022).

³⁶¹ Google, "Find & control your Web & App Activity" <https://support.google.com/accounts/answer/54068?hl=en&co=GENIE.Platform%3DAndroid> (accessed December 20, 2022). This page used to be titled "See & control your Web & App Activity." Google in its Responses to Interrogatory Nos. 6-8 made available by Bates numbers a list of prior versions of this WAA Help Page. I reviewed these prior versions of this page. Google's representations regarding WAA were consistent throughout the class period.

Rodriguez v. Google

315. The page hides important information about how Google collects and saves information. Specifically, it fails to explicitly distinguish between the collection and saving of web and app activity data within one's "Google Account" and the collection and saving of the same data outside of one's "Google Account." It fails to distinguish between individual users and the Google accounts of those users. It fails to inform users that Google's internal definition of a "Google Account" excludes several Google-created and -controlled identifiers that Google uses to track users across their app activity. It also fails to explicitly counter the negative implication of its promise of control.

316. For example, the subject title for all three versions of the page (one each for desktop, Android, and iOS platforms) states that the information will allow the user to "find and control" their "web and app activity." Specifically, the text promises that "If Web & App Activity is turned on, your searches and activity from other Google services are saved in your Google Account," and that if the user doesn't want their activity to be saved, they "can turn Web & App Activity off or delete past activity at any time."³⁶² The negative implication of these assurances is that disabling WAA and sWAA will disable Google's collection, retention, and utilization of data about one's online activity. This implication is false.

317. The WAA Help Page further states:

When Web & App Activity is on, Google saves information like:

- Searches and other things you do on Google products and services, like Maps and Play
- Your location, language, IP address, referrer, and whether you use a browser or an app
- Ads you click, or things you buy on an advertiser's site
- Information on your device like recent apps or contact names you searched for³⁶³

318. The page also states:

When Web & App Activity is on, you can include additional activity like:

- Sites and apps that partner with Google to show ads
- Sites and apps that use Google services, including data that apps share with Google
- Your Chrome browsing history
- Android usage & diagnostics, like battery level and system errors.

To let Google save this information:

- Web & App Activity must be on.

³⁶² Google, "Find & control your Web & App Activity," *Google Account Help*, <https://support.google.com/accounts/answer/54068> (accessed December 20, 2022).

³⁶³ Google, "Find & control your Web & App Activity," *Google Account Help*, <https://support.google.com/accounts/answer/54068> (accessed December 22, 2022).

Rodriguez v. Google

- The [sWAA] box next to “Include Chrome history and activity from sites, apps, and devices that use Google services” must be checked.³⁶⁴

319. Google’s description of its privacy controls as “on/off” is inaccurate with respect to WAA and sWAA, since even when set to “off,” Google collects and stores data relating to users’ activity on apps that use Google services like Google Analytics for Firebase. Google has admitted that WAA “functions independently from Google Analytics for Firebase” such that “a user turning off [WAA] does not prevent” Google from collecting and saving data by way of Google Analytics for Firebase.³⁶⁵

320. These are all forms of sneaking. Google tells users that if they turn WAA/sWAA on, Google will save their web and app activity data, including activity on third-party sites, to their account. Google tells users that if they turn WAA/sWAA off, Google will not save data to their account. Google never explicitly tells users the critical fact that even if they turn WAA/sWAA off, Google will save data about their online activity outside of their account. Google also does not tell users that even if they turn WAA/sWAA off, Google will save their app activity data along with a persistent, Google-created and -controlled identifier like AdID. To the contrary, the WAA Help Page elsewhere states that “To let Google save this information [i.e., data relating to activity on apps that use Google services like Firebase, AdMob, and Ad Manager] Web & App Activity must be on” without providing any qualifying information about where or how Google will save the data. Google engages in “sneaking” by failing to inform users that Google will save the data regardless, just in a different form and in a different place.

321. Even those in the industry can be fooled. A 2022 *CNet* article, titled “Is Google tracking you? Here’s how to check and stop it,” directs users to “Stop Google from collecting your web and app activity” by turning off the WAA controls, with no further discussion of the data collection that continues to occur even after this is done.³⁶⁶

322. Google’s employees were fooled, too. In his deposition, Chris Ruemmler stated that he had been unclear about what exactly WAA controlled in 2019, then again in 2020, even as he was involved in discussions about the name “Web & App Activity” and the disclosures made to users about WAA.³⁶⁷ He described how, when the WAA control is turned off, user activity continues to be collected by Google—a concept that he, a Google software engineer, had not previously understood:

“[B]ack before I had more knowledge about the way WAA works...I thought at that time if the opposite of on and off, if it was off, well, we just didn’t, you know, send any of this data to Google. But that’s not right. It’s really you don’t

³⁶⁴ Google, “Find & control your Web & App Activity,” *Google Account Help*, <https://support.google.com/accounts/answer/54068> (accessed December 22, 2022).

³⁶⁵ Google’s Resp. to Request for Admission 2.

³⁶⁶ Kelsey Fogarty and Zachary McAuliffe, “Is Google tracking you? Here’s how to check and stop it,” *CNET*, <https://www.cnet.com/tech/services-and-software/is-google-tracking-you-heres-how-to-check-and-stop-it> (December 3, 2022).

³⁶⁷ Ruemmler Tr. 155:16-25; 156:1-7.

Rodriguez v. Google

associate the data that's sent to Google with a GAIA ID...the internal identifier at Google that identifies an account with an individual.”³⁶⁸

“I had the recollection that, you know, off—a light is on, a light is off; right? You know, that's the opposite behavior. And so I think I had a misconception that when WAA was off, there was no logging performed, which was not the right, you know, understanding.”³⁶⁹

323. Mr. Ruemmler likewise testified that based on his review of the WAA Help Page, “I didn't know the data was saved anonymously even with WAA off.”³⁷⁰

324. Mr. Ruemmler encouraged revisions to the WAA Help Page in a July 2019 email, warning that “[t]he WAA and other controls imply we don't log the data, but obviously we do. We need to change the description to indicate even with the control off, Google retains this data and uses it for X purposes” and to “indicate that WAA off is identical to being not logged into your account (data logged, but not tied to your account).”³⁷¹

325. Mr. Ruemmler reiterated his concerns about the WAA Help Page later that year in another email to colleagues: “Isn't WAA off supposed to NOT log at all? At least that is what is implied from the WAA page [hyperlink]. So, if WAA is off, how are we [Google] able to log at all?”³⁷²

326. The inaccurate nature of Google's representations is also reflected in Plaintiffs' testimony.

327. Plaintiff Sal Cataldo testified that Google's disclosures about WAA list “what gets saved,” then state that, “To let Google save this information, Web & App Activity must be on.” Mr. Cataldo continued: “So if I don't want to let Google save that information, I turn it off.” Mr. Cataldo summarized his understanding as follows: “That's pretty simple. That's pretty elementary.” When asked by Google's counsel whether he would believe that his privacy were being invaded if the collected “data is anonymized,” Mr. Cataldo responded in part by noting that Google's disclosures refer to “what's saved, information. Not information in a way that portrays it as you” In other words, Mr. Cataldo understood that the disclosures are not limited to Google's collection of identified information.

328. Plaintiff Julian Santiago likewise testified: “If I had web-and-app activity on, I would be giving Google permission to collect my private—my information. I have web-and-app activity off. Therefore, I did not give them permission.”³⁷³ He continued: “They make a very clear in the web-and-app activity page that web-and-app activity must be on for all those things that they list out, those bullet points to track. So if it's off, they're not tracking.”³⁷⁴

³⁶⁸ Ruemmler Tr. 72:22-25, 73-1-3; 74:13-14.

³⁶⁹ Ruemmler Tr. 135:20-25, 136:1.

³⁷⁰ Ruemmler Tr. 79:18-20.

³⁷¹ GOOG-RDGZ-00024709 at -10-11.

³⁷² GOOG-RDGZ-00130381.

³⁷³ Santiago Tr. 39:12-15.

³⁷⁴ Santiago Tr. 145:11-15.

Rodriguez v. Google

329. Plaintiff Susan Lynn Harvey likewise testified: “When [WAA] is on, you can include...sites and apps that use Google services.... And to let Google save this information, I’m supposed to have turned it on. And I turned it off so that couldn’t be done.”³⁷⁵

330. Plaintiff Anibal Rodriguez likewise testified: “[W]hen WAA is on, it does say...you can include additional activities.... Also and it does say here: ‘To let Google save this information, Web & App Activity must be turned on.’ So if I say I don’t want it on, I would assume that everything you’re telling me that comes along with it being on would be turned off.” Mr. Rodriguez later explained: “Google says that, in order for me to let them save the information, that Web & App Activity must be turned on. And since, any of that information there should not be collected if it’s turned off.” He also described how “I feel that that I’m being harmed by Google... not doing what they said they’re going to do, which is not collect my information if my WAA... is off.”

331. As Google’s Vice President of Marketing Cassidy Morgan put it in a 2020 interview, “What drives users crazy is when we do stuff that feels clandestine” and “when we do stuff that they don’t have the ability to have an exit door.”³⁷⁶ Google’s systems do not provide an exit from collection of data from users’ app usage and other online activity, even as they claim to provide such an exit by means of the WAA and sWAA controls.

11.2. Disclosures Accompanying the WAA and sWAA Toggles, including the “Activity Controls” Page, Exemplify Dark Patterns

332. The WAA Help Page is not the only WAA disclosure that exhibits dark patterns. Google also uses dark patterns alongside the WAA and sWAA toggles themselves, including “sneaking.”

333. Since May 25, 2018, the Google Privacy Policy has promised users that “across our services, you can adjust your privacy settings to control what we collect and how your information is used.” The Privacy Policy also contains a section within “Privacy controls” called “Activity controls,” promising that users can “Decide what types of activity you’d like saved in your account.” A hyperlink inviting users to “Go to Activity Controls” brings users to the “Activity controls” page where users can switch WAA and sWAA on or off.³⁷⁷ As with the WAA Help Page, this provision in the Privacy Policy fails to inform users that these “activity controls” will not prevent Google from collecting and saving data about users’ web and app activity, and that the controls merely decide whether the data will be explicitly associated with the user’s Google Account. Beginning on February 10, 2022, Google began to state that sWAA “lets you control whether information about your activity on other sites, apps, and devices that use Google services...is saved in your Google Account,” but still does not disclose that it saves data anywhere else. Moreover, that quoted language is a hyperlink that leads to the WAA Help Page, which I discussed in Section 11.1.

334. In August 2019, Chris Ruemmler commented regarding Google’s “Activity Controls” page: “I don’t see how this text can’t need modification. An ‘on/off’ toggle means the off state is

³⁷⁵ Harvey Tr. 83:15-22.

³⁷⁶ GOOG-RDZ-00188868 at -87.

³⁷⁷ Google, “Activity controls,” *Google Account*, <https://myactivity.google.com/activitycontrols> (accessed January 31, 2023).

Rodriguez v. Google

the opposite of the on state. If the on state is we log your activity, the off state is we don't log your activity.”³⁷⁸ I agree. Off should mean off. Nonetheless, Google’s “Activity Controls” page has never disclosed that Google will collect and save information relating to users’ activity on non-Google apps even when WAA and/or sWAA are turned off. To the contrary, this page states that WAA “saves your activity on Google sites and apps....” and that sWAA enables you to “include...activity from sites, apps, and devices that use Google services.”³⁷⁹ There is also a “Learn more” hyperlink that brings users to the WAA Help Page.

335. If a user chooses to turn off WAA from the “Activity Controls” page, a pop-up appears which states that “Web & App Activity saves the things you do on Google sites, apps, and services.”³⁸⁰ If the user elects to turn off sWAA from this page, another pop-up appears which states that sWAA “saves your activity from sites, apps, and devices that use Google services,” including “activity from sites and apps that partner with Google to show ads.”³⁸¹ Once again, these disclosures fail to inform users that Google will collect and save the data regardless of whether WAA and sWAA are on or off. These disclosures also fail to inform users that Google will save the data alongside a persistent, Google-created and -controlled identifier like AdID.

336. Google’s “Activity Controls” page also contains a hyperlink to the page “Manage all Web & App Activity,” which states, “Your Web & App Activity includes the things you do on Google services, like Maps, Search, and Play. It can also include things you do on sites, apps, and devices that use Google services.”³⁸² The “Manage all Web & App Activity” page is another place where users can toggle WAA and sWAA on or off. It is also another place where Google fails to inform users that switching off WAA or sWAA does not prevent Google from collecting and saving their data, or associating it with a Google identifier.

337. The “Activity Controls” page also contains the statement: “You control what data gets saved to your account,” underneath which is a “Learn more” hyperlink leading to the Google Safety Center page, which describes Google’s Activity Controls as tools that “allow you to switch the collection and use of data on or off.”³⁸³ One of those tools is WAA. In fact, however, WAA is not a true on/off switch; Google will collect and save users’ data regardless—just in a different form.

338. Users with an Android device can also access the “Activity Controls” page through the “Privacy” submenu within the Settings menu. There, users can click on the text “Activity controls” to “Choose the activities and info you allow Google to save.” That click leads to a screen titled “Activity controls” which contains the same information as the “Activity controls”

³⁷⁸ GOOG-RDGZ-00130322.

³⁷⁹ GOOG-RDGZ-00208190. This document lists prior versions of the disclosures as well. None disclosed the collection at issue in this case, namely, Google’s collection of app-activity data from users who had switched off WAA and/or sWAA off. Rather, this page has since 2015 represented that sWAA controls whether “history” from “apps” is “save[d].”

³⁸⁰ GOOG-RDGZ-00208190 at -91.

³⁸¹ GOOG-RDGZ-00208190 at -93.

³⁸² Google, “Activity controls,” *Google Account*, <https://myactivity.google.com/activitycontrols> (accessed January 31, 2023).

³⁸³ Google, “Privacy controls,” *Google Safety Center*, <https://safety.google/privacy/privacy-controls> (accessed January 31, 2023).

Rodriguez v. Google

page discussed just above, including the option to toggle WAA and sWAA on or off.³⁸⁴ The Android “Activity controls” screen also has a “Learn more” hyperlink that leads to a screen which mirrors the WAA Help Page, discussed above.

339. None of these Google disclosures inform users that Google collects, saves, and uses their app activity data even when they exercise their right to control their data by way of the Google “privacy controls” WAA and sWAA. To the contrary, Google has uniformly stated that users are in control of Google’s collection of their data, and has invited them to exercise that control by using WAA and sWAA.

11.3. Google Statements about Privacy and User Control Exemplify Dark Patterns

340. In Colin Gray’s taxonomy, “interface interference” is defined as “any manipulation of the user interface that privileges specific actions over others, thereby confusing the user or limiting discoverability of important action possibilities... Interface interference manifests as numerous individual visual and interactive deceptions, and is thus our most involved strategy with three subtypes: hidden information, preselection, and aesthetic manipulation.” Aesthetic manipulation is defined as “instances where manipulation of aesthetic characteristics leads to misunderstanding of hierarchy, content type, or unrealistic sense of urgency.”³⁸⁵

341. The FTC defines the dark pattern of “misdirection” as “using style and design to focus users’ attention on one thing in order to distract their attention from another.”³⁸⁶

342. In the EU’s taxonomy, “emotional steering” is a subcategory of “stirring.” It is defined as “Using wording or visuals in a way that confers the information to users in either a highly positive outlook, making users feel good or safe, or in a highly negative one, making users feel scared or guilty. Influencing the emotional state of users in such a way is likely to lead them to make an action that works against their data protection interests.”³⁸⁷ This roughly corresponds to aesthetic manipulation, a subcategory of interface interference.

343. Google’s behavior around privacy controls in general and WAA/sWAA in particular exemplifies interface interference, misdirection, and emotional steering. Google repeatedly reassures users that they are in control of their privacy, and over the data that Google collects and saves. These substantial-sounding assurances reflect the objective of helping users to feel comfortable and to make privacy choices deemed most favorable by Google.³⁸⁸

³⁸⁴ Fourth Am. Compl., Dkt. 289 ¶ 90; Google’s Answer, Dkt. 305 ¶¶ 90-93.

³⁸⁵ Colin M. Gray, et al., “The dark (patterns) side of UX design,” CHI 2018, Montreal, Quebec, Canada, <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (April 21-26, 2018).

³⁸⁶ US Federal Trade Commission, “Bringing dark patterns to light,” Staff Report, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (September 2022).

³⁸⁷ Andrea Jelinek, et al., “Dark patterns in social media platform interfaces: How to recognise and avoid them,” Version 1.0, European Data Protection Board, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (14 March 2022).

³⁸⁸ GOOG-RDZ-00149527 at -29.

Rodriguez v. Google

344. For example, the current version of the Google privacy policy references the WAA Help Page, a link to which is embedded in the text of the “Activity Controls” description:

“[I]f you have Web & App Activity turned on, your searches and activity from other Google services are saved in your account so you can get more personalized experiences like faster searches and more helpful app and content recommendations. Web & App Activity also has a subsetting that lets you control whether **information about your activity on other sites, apps, and devices that use Google services**, such as apps you install and use on Android, is saved in your Google Account and used to improve Google services.”³⁸⁹ (emphasis added; bolded phrase links to WAA Help Page)

345. This text fails to make the subtle but meaningful distinction that turning off the WAA and/or sWAA settings does not prevent Google, by means of Google services like Firebase, AdMob, and Ad Manager, from collecting and saving information relating to your activity on third-party apps you install and use. It also does not disclose that, even when WAA or sWAA is off, Google will continue to save app activity data alongside persistent, Google-created and -controlled identifiers like AdID.

346. Moreover, as noted above, the Google Privacy Policy has, since May 25, 2018, promised that “across our services, you can adjust your privacy settings to control what we collect and how your information is used.” The Privacy Policy defines “Google services” to include “[p]roducts that are integrated into third-party apps and sites, like ads [and] analytics,” and describes Google’s “Activity Controls” (which include WAA and sWAA) as “Privacy controls,” directing users to “Go to Activity controls” where they can toggle WAA and sWAA to off.³⁹⁰ Google thus (falsely) assures users that they can use WAA and sWAA to control whether Google collects their data in the context of activity on non-Google apps.

347. Similarly, on its page, “Our privacy and security principles,” Google states, “every Google Account is built with on/off data controls, so our users can choose the privacy settings that are right for them. And as technology evolves, our privacy controls evolve as well, ensuring that privacy is always an individual choice that belongs to the user.”³⁹¹

348. Google’s promises to users are also made via public relations efforts by product managers and executives, with blog posts, op-eds and public presentations that uniformly seek to reassure the public of Google’s benevolence and users’ ability to control the collection, storage, and use of records of their online activity by means of the activity controls.

349. Consider the above-cited Congressional testimony by Google CEO Sundar Pichai, who responded to the chairman’s opening question about the ubiquity of Android data collection by asserting that its extent is “a choice users make.”³⁹² In May 2019, Mr. Pichai broadcast this

³⁸⁹ Google, “Privacy policy,” <https://policies.google.com/privacy> (December 15, 2022).

³⁹⁰ Google, “Activity controls,” *Google Account*, <https://myactivity.google.com/activitycontrols> (accessed January 31, 2023).

³⁹¹ Google, “Our privacy and security principles,” <https://safety.google/principles> (accessed December 23, 2022).

³⁹² C-SPAN, “LIVE: Google CEO Sundar Pichai testifies on data collection (C-SPAN),” YouTube, <https://www.youtube.com/watch?v=WfbTbPEEjXI> at 43:10 (December 11, 2018).

Rodriguez v. Google

message again in a *New York Times* op-ed extolling the company's commitment to privacy and user control: "To make privacy real, we give you clear, meaningful choices around your data."³⁹³

350. The following year, before another congressional hearing on the power of online platforms, Pichai continued to emphasize Google's commitment to "keeping your information safe, treating it responsibly, and putting you in control of what you choose to share. We also never sell user information to third parties."³⁹⁴

351. Google's public emphasis on users' ability to control collection of data generated by their online activity is supported by its internal research. For example, one study reported that "3/8 participants mentioned that seeing the message about control placed so prominently on the Home page is reassuring," and that the "'You're in control' message helps build trust between users and Google."³⁹⁵

352. Google's blog, *The Keyword*, regularly features articles touting the company's commitment to user privacy and control, by product managers, including Guemmy Kim, Greg Fair, Jan Hannemann, Justin Schuh, and Eric Miraglia, and Vice President of Product Privacy Rahul Roy-Chowdhury:

- "Google builds simple, powerful privacy and security tools that keep your information safe and put you in control of it."³⁹⁶
- "Collectively, these tools make it easy for you to control your privacy and security from any device."³⁹⁷
- "You—and only you—can view and control the information in My Activity."³⁹⁸
- "[E]asy-to-use privacy features and controls have always been built into our products.... As the number of Google products has grown, we're making it even easier to find these controls."³⁹⁹

³⁹³ Sundar Pichai, "Google's Sundar Pichai: Privacy should not be a luxury good," *New York Times*, <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html> (May 7, 2019).

³⁹⁴ US House of Representatives, "Written testimony of Sundar Pichai, Chief Executive Officer, Alphabet, Inc.," Online platforms and market power, part 6: Examining the dominance of Amazon, Apple, Facebook, and Google," Hearing Before the Subcommittee on Antitrust, Commercial, and Administrative Law of the House Committee on the Judiciary, <https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-PichaiS-20200729.pdf> (July 29, 2020).

³⁹⁵ GOOG-RDGZ-00117318 (Tab 1, Row 17).

³⁹⁶ Guemmy Kim, "Keeping your personal information private and safe—and putting you in control," *The Keyword*, Google, <https://blog.google/topics/safety-security/privacy-security-tools-improvements> (June 1, 2015).

³⁹⁷ Guemmy Kim, "Celebrating My Account's first birthday with improvements and new controls," *The Keyword*, Google, <https://blog.google/technology/safety-security/celebrating-my-accounts-first-birthday> (June 1, 2016).

³⁹⁸ Greg Fair, "Improving our privacy controls with a new Google dashboard," *The Keyword*, Google, <https://www.blog.google/topics/safety-security/improving-our-privacy-controls-new-google-dashboard> (September 8, 2017).

³⁹⁹ Eric Miraglia, "Privacy that works for everyone," *The Keyword*, Google, <https://blog.google/technology/safety-security/privacy-everyone-io> (May 7, 2019).

Rodriguez v. Google

- “To help you better understand and take control of your Google Account, we’ve made all your privacy options easy to review with our new intuitive, user-tested design.”⁴⁰⁰
- “Technology that publishers and advertisers use to make advertising even more relevant to people is now being used far beyond its original design intent—to a point where some data practices don’t match up to user expectations for privacy.”⁴⁰¹
- “We do not sell your personal information to anyone and give you transparency, choice and control over how your information is used.”⁴⁰²

353. In reality, there is not any “control” that will allow users to entirely prevent Google from collecting app-activity data that Google collects. But through public statements like those just above, Google hid this fact from the public.

354. In 2016, Google technical writer David Warren acknowledged that Google is “intentionally vague” about the distinction between data saved in a user’s Google Account and data “collected outside of their Google Account.”⁴⁰³ Google’s phrase that “more information will be visible in your Google Account,” Warren noted, is “vague about where the data that wasn’t visible was.” In response to those comments, Jonathan McPhie, Director of Product Management, remarked: “Our definition of ‘collect’ is more like ‘stored’.... From that perspective sWAA...is more about moving data around and not about ‘collecting’ more data.” Neither is it about collecting less data.

355. In a subsequent discussion of language to be used in a new edition of Privacy Advisor (an Android feature that enables users to adjust their privacy settings), Rajni Posner, Google’s Brand Strategist for User Trust Marketing, suggested rewording the phrase “what data Google saves and uses across Google services” to the passive voice, as “what data is saved and used across Google services.” David Warren’s reply illustrates the nuances of language designed to engender a false sense of agency on the part of the end user with respect to the matter of privacy: “I like Rajni’s suggestion. It’s true that we try to use active voice as a rule, but I like her construction in this case because of the slight ambiguity it introduces. I’ve even written some strings in the past that make the user the agent when saving data, like “Choose what data you want to save...” If we’re pushing the control story, then, in a sense, it’s the user choosing what data to save, so let’s remove Google as the agent in this case.”⁴⁰⁴

356. The deposition testimony from the named Plaintiffs in this case illustrates the effect of Google’s use of dark patterns, including “Aesthetic Manipulation,” in its statements about privacy and user control.

⁴⁰⁰ Jan Hannemann, “More transparency and control in your Google account,” *The Keyword*, Google, <https://blog.google/technology/safety-security/more-transparency-and-control-your-google-account> (June 21, 2018).

⁴⁰¹ Justin Schuh, “Building a more private web,” *The Keyword*, Google, <https://www.blog.google/products/chrome/building-a-more-private-web> (August 27, 2019).

⁴⁰² Rahul Roy-Chowdhury, “Data Privacy Day: Seven ways we protect your privacy,” *The Keyword*, Google, <https://blog.google/technology/safety-security/data-privacy-day-seven-ways-we-protect-your-privacy> (January 28, 2020).

⁴⁰³ GOOG-RDGZ-00149701 at -02.

⁴⁰⁴ GOOG-RDGZ-00207105 at -06.

Rodriguez v. Google

357. For example, Plaintiff Julian Santiago testified: “[R]ight on the first page of the privacy policy, Google is letting me know what they are putting me in control of my information. And if I opt out of sharing that information of Google collecting that information, then they shouldn’t be collecting and tracking that information.”

358. Plaintiff Susan Lynn Harvey likewise testified: “I was offered an option to be able to turn off data collection to where it wouldn’t be saved or used or stored or anything, and that wasn’t done.”

359. Notwithstanding Google’s promises, Google employees have confirmed that there is no way for users to prevent Google from collecting and saving information relating to their activity on non-Google apps that use Google services such as Firebase. Consider this exchange from the deposition of Eric Miraglia:

Counsel: So I’m just trying to ask at a more...general level, not focusing only on Firebase or...Analytics, but whether you’re aware of any Google control that would just full stop Google from collecting any data about a user’s app activity.

Witness: I’m not aware of any setting that—that’s shaped exactly the way you described it.⁴⁰⁵

360. There is also no way for users to actually delete so-called “pseudonymous” data that Google has collected. Greg Fair, formerly Google’s Product Manager for Privacy and Data Protection, has testified that “I’m not aware of a specific control that the user can delete something from Google. The controls that we have in in the My Activity space talk about deleting a piece of data from your account.”⁴⁰⁶

361. Google prioritizes creating the perception of offering users “control”—as opposed to delivering on that promise.

362. Google’s behavior toward enterprise customers also calls to mind dark patterns. In March 2022, Google removed the WAA control from the administrator console for Google Workspace, a suite of enterprise services including Gmail, Calendar, Docs, Contacts, Drive, Google Chat, and Keep; added a new “Google Workspace Search History” setting to individual users’ My Activity page; and switched that setting on by default, even if their organization’s Workspace administrator had previously disabled the WAA setting.⁴⁰⁷ As summarized by technical journalist Ron Amadeo, “for paying Workspace users, Search History will now cover usage data for Workspace stuff, while Web & App Activity will cover every other Google product that isn’t

⁴⁰⁵ Miraglia Tr. 96:15-97:6.

⁴⁰⁶ Fair Tr. 79:6-10; *see also* Miraglia Tr. 134:14-137:19.

⁴⁰⁷ Hacker News, “Google to turn on activity tracking for many users who turned it off,” <https://news.ycombinator.com/item?id=30171800> (February 1, 2022).

Rodriguez v. Google

specifically listed in the Workspace terms.”⁴⁰⁸ Additionally, the new ‘Search History’ setting introduced by Google doesn’t cover Google Search history.

363. Google’s email notifying Workspace administrators of the change acknowledged that some enterprise customers chose to disable WAA.⁴⁰⁹ That decision, nonetheless, was overridden under the new system. Clearly, Google could have simply retained the previous administrator setting for “Google Workspace Search History,” but chose not to do so. Instead, it chose a plan of action that promised to inconvenience individual end users made newly responsible for privacy settings for enterprise services, and to simultaneously create a new stream of ostensibly “consented” user data.⁴¹⁰

11.4. Google’s WAA Controls for Location Privacy Exemplify Dark Patterns

364. In Gray’s taxonomy, “Hidden Information” is a subcategory of “Interface Interference,” defined as “options or actions relevant to the user but not made immediately or readily accessible.”⁴¹¹

365. In the EU’s taxonomy, “conflicting information” is a subcategory of “left in the dark.” It is defined as “Giving pieces of information to users that conflict with each other in some way.”⁴¹² This roughly corresponds to hidden information.

366. Google’s use of two different controls for the privacy of location information is an example of hidden information.

367. In 2022, an Australian federal court fined Google \$42.6 million (US dollars) for making misleading representations about the collection and use of location data on Android phones. The Australian investigation targeted Google’s practice of implying to users that the “Location History” setting was the sole control by which users could authorize Google to collect their location data. In fact, WAA also controlled that collection. Both had to be set to “off,” and WAA was turned on by default.⁴¹³

⁴⁰⁸ Ron Amadeo, “Google Workspace to strip privacy control from admins, re-enable tracking,” *Ars Technica*, <https://arstechnica.com/gadgets/2022/02/confusing-google-workspace-privacy-change-will-re-enable-tracking-for-users> (February 2, 2022).

⁴⁰⁹ Google Workspace Team, “[Action Advised] Review new Workspace search history control for users [email],” <https://pastebin.com/raw/5ayJTDDp> (January 31, 2022).

⁴¹⁰ Google Workspace, “Google Workspace (online) agreement,” https://workspace.google.com/terms/2013/1/premier_terms.html (October 6, 2020).

⁴¹¹ Colin M. Gray, et al., “The dark (patterns) side of UX design,” CHI 2018, Montreal, Quebec, Canada, <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (April 21-26, 2018).

⁴¹² Andrea Jelinek, et al., “Dark patterns in social media platform interfaces: How to recognise and avoid them,” Version 1.0, European Data Protection Board, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (14 March 2022).

⁴¹³ Australian Competition and Consumer Commission, “Google LLC to pay \$60 million for misleading representations,” <https://www.accc.gov.au/media-release/google-llc-to-pay-60-million-for-misleading-representations> (August 12, 2022).

Rodriguez v. Google

368. In October 2022, the Arizona Attorney General announced an \$85 million settlement with Google for the same issue, calling the practice of requiring two coordinated settings for disabling location tracking “deceptive and unfair.”⁴¹⁴ And in November, Google settled with the attorneys general of forty other states for \$391.5 million for the same reason.⁴¹⁵

369. Google employees had recognized the problems with this deceptive practice. Danny Sullivan, Google’s Public Liaison for Search, observed, “This is so convoluted how we do it that I have to point to our help page rather than the actual control—and then hope people can scroll to the right place on the help page to discover that while we have one control for Location History in Activity Controls, they have to jump to Google Maps Timeline and figure out they should click on the small trash can icon. I sure didn’t get that, at first. [...] Overall, it’s still mind-numbing to try and figure this all out even when you work at Google.”⁴¹⁶

11.5. Google’s WAA/sWAA “Consent Bump” Prompt Exemplifies Dark Patterns

370. In Colin Gray’s taxonomy, “nagging” is defined as “a minor redirection of expected functionality that may persist over one or more interactions. Nagging often manifests as a repeated intrusion during normal interaction, where the user’s desired task is interrupted one or more times by other tasks not directly related to the one the user is focusing on. Nagging behaviors may include pop-ups that obscure the interface, audio notices that distract the user, or other actions that obstruct or otherwise redirect the user’s focus”⁴¹⁷

371. The FTC defines the dark pattern of “nagging” as “asking repeatedly and disruptively if a user wants to take an action or making a request that doesn’t let the user permanently decline—and then repeatedly prompting them with the request.

372. In the EU’s taxonomy, “continuous prompting,” a subcategory of “overloading,” corresponds to nagging. It is defined as: “when users are pushed to provide more personal data than necessary for the processing purposes or to consent to another use of their data, by being repeatedly asked to provide additional data and offered arguments why they should provide it. Users are likely to end up giving in, i.e. accepting to provide more data or to consent to another processing, as they are wearied from having to express a choice each time they use the platform.”⁴¹⁸

⁴¹⁴ Angela Cordoba Perez and Jose R. Gonzalez, “Arizona announces \$85M settlement with Google for allegedly tracking users’ location deceptively,” *Arizona Republic*, <https://www.azcentral.com/story/news/local/arizona-breaking/2022/10/04/mark-brnovich-announces-85-m-settlement-google-after-investigation/8176001001> (October 4, 2022).

⁴¹⁵ Tony Foley, “Google settles with state AGs over location-tracking,” *Cybersecurity Policy Report*, <https://www.vitallaw.com/news/cybersecurity-policy-report-google-settles-with-state-ags-over-location-tracking-nov-14-2022/cspd01c4651b62a7664db7a65684bef2600b6c> (November 14, 2022).

⁴¹⁶ GOOG-RDZ-00041092-3.

⁴¹⁷ Colin M. Gray, et al., “The dark (patterns) side of UX design,” CHI 2018, Montreal, Quebec, Canada, <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (April 21-26, 2018).

⁴¹⁸ Andrea Jelinek, et al., “Dark patterns in social media platform interfaces: How to recognise and avoid them,” Version 1.0, European Data Protection Board, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (14 March 2022).

Rodriguez v. Google

373. These tactics are also exemplified by Google’s practice of repeatedly asking users who turn off location settings to turn them back on again. For example, Google Maps users who disable Location Accuracy, which uses wireless and mobile networks and unspecified sensors to refine its estimates of users’ location, are repeatedly prompted to turn on the setting even though Google Maps works perfectly well using GPS.

374. Nagging also applies to Google’s efforts to persuade users to turn on WAA and sWAA. For example, Google’s internal “Narnia 2.0” project involved the development of an updated WAA/sWAA consent screen, along with a campaign to encourage users to enable their WAA/sWAA settings if they had not already done so.

375. As explained by Eric Miraglia, “users would be presented with a screen where they would see what the settings were currently set to, and they’d have a chance to update their preferences.... [A]s soon as you signed in to your Google account, you would see that screen.... [W]e also used push notifications as another mechanism.”⁴¹⁹

376. In an internal email discussion, Eric Miraglia noted that “sWAA was off by default from 2014, when it was introduced, until mid-2016, when Narnia 2.0 came along.”⁴²⁰ According to Mr. Miraglia, Narnia 2.0 “introduced a consent flow that specifically reminded users about how these settings and others worked and allowed users who didn’t have them on to turn them on.... The general direction of Narnia 2.0...was to refine the way our settings worked to give users more control and simpler control over the way data was collected and used.”⁴²¹

377. Google discussed this “consent bump” (that is, the screen that enables the user to give or revoke consent⁴²²) in a filing in *Calhoun v. Google, LLC*, echoing Mr. Miraglia’s testimony in this case. The *Calhoun* submission states that “Google Account holders as of June 2016...were shown the Consent Bump Agreement upon logging into their accounts.”⁴²³ Another *Calhoun* submission explained: “Beginning in July 2016, existing Google Account holders were taken directly to the Consent Bump Agreement upon signing into their Google Account on their desktop.”⁴²⁴

378. That is, beginning in July 2016 (before the start of the class period in this case), Google began prompting account holders whose WAA or sWAA controls had previously been “off” to turn them both on, when they signed into their Google account. A document produced in the

⁴¹⁹ Miraglia Tr. 57:23-58:1; 60:2-5; 8-16.

⁴²⁰ GOOG-RDGZ-00145259, cited in Miraglia Tr. 55:10-12.

⁴²¹ Miraglia Tr. 57:23-25, 58:1; 72:10-13.

⁴²² Miraglia Tr. 80:3-6.

⁴²³ Case No. 20-cv-05146 (N.D. Cal.), Dkt. 395 at 6.

⁴²⁴ Case No. 20-cv-05146 (N.D. Cal.), Dkt. 395-1 at 8. The same court filing addresses Google’s “New Account Creation Agreement” that was “shown to users beginning June 2016.” At 18. Like the consent bump, and the other disclosures addressed in this report, the consent flow for the New Account Creation agreement did not disclose that Google collects and saves data relating to users’ interactions with non-Google apps regardless of whether WAA or sWAA are on or off. To the contrary, this agreement featured WAA alongside Google’s promise that “You’re in control of the data we collect & how it’s used.” At 24.

Rodriguez v. Google

instant case depicts the “flow” displayed to users with the consent bump notice.⁴²⁵ The first screen described WAA, Chrome Sync and Ads Personalization in terms of benefits to users, and prompted users to select “Choose I AGREE to turn these features on or MORE OPTIONS for more choices.” The “AGREE” option was presented in the lower right corner with a blue button, drop-shaded to simulate popping out from the screen, and far more prominent than the text link to “More Options.” The “More Options” screen featured three radio buttons with the text, “No changes—continue to Gmail,” “No changes—review key privacy settings more fully,” and “Yes I’m in—turn on these new features.” Nowhere on either screen was the user’s current WAA/sWAA status displayed, leaving the meaning of “No changes” ambiguous. Users seeking that information would have to click on the second button, “No changes—review key privacy settings more fully,” to proceed to the “Privacy Checkup” page.

379. Both visually and verbally, the Narnia 2.0 consent flow subtly discouraged users from disabling their account’s WAA and sWAA settings. A 2016 document by Google technical writer David Warren notes that the first objective of the new WAA/sWAA consent bump was not to clearly inform users of the full scope of data collection, but to “Help users feel comfortable choosing ACCEPT.” Mr. Warren then listed “Preferred user actions [...] from most to least favorable”:

- “ACCEPT: The interface is designed to get people to choose ACCEPT. A user who chooses ACCEPT is agreeing to have Google:
 - Turn on or leave on the existing Google Web & App Activity setting.
 - Turn on the new Apply my Signed-in Ads Choices Everywhere setting. [early user-facing name for sWAA]
- CUSTOMIZE → CHECK BOTH SETTINGS: A user who chooses to customize is prompted with both settings and checkboxes that allow the user to opt into these settings. If a user checks both boxes and clicks SAVE, that has the same effect as a different user who choose ACCEPT on the top page.
- CUSTOMIZE → CHECK 1 SETTING
- CUSTOMIZE → CHECK NEITHER SETTING”

380. Warren continued: “A user should be able to read the consent bump in layers from little to more detail. We’d like the user to feel comfortable clicking ACCEPT as quickly as possible. In other words, if the user stops at layer 1 [i.e., the page title], and clicks ACCEPT, that’s fine.... [M]any users will blindly choose ACCEPT, having already bought into a relationship with Google based on trust.”⁴²⁶ The wording of titles, page summaries, and paragraphs, Warren noted, should all be focused on making users feel good about Google; they should be “reassuring to the user” and “as simple as possible to contribute to the sense of simplicity and transparency we want the user to feel.” A secondary “CUSTOMIZE” page “might offer more details around each setting definition, but even if the explanation isn’t any more detailed, the page allows the user to modify the 2 settings individually, an important means to convey a sense of control.” Making the option to accept Google’s preferred option on a first screen, and requiring users to click through to a secondary screen to reject that option, is also an important means to steer users towards Google’s preferred outcome.

⁴²⁵ GOOG-RDGZ-00149771.

⁴²⁶ GOOG-RDGZ-00149527 at -29-30.

Rodriguez v. Google

381. Sneaking also occurs through close parsing of language used in the WAA/sWAA disclosures, and by omission of relevant information. In a 2019 email exchange, software engineer Chenjun Wu stated, “We have a few existing systems like online web conversion tracking and store sales direct that do not respect WAA or sWAA today, and enforcing that will have significant impact on the product.” Fellow engineer Uwe Bubeck replied, “conversion tracking wouldn’t be generally subject to sWAA [...] [T]hose controls would only apply if conversions were also used for subsequent personalization. [...] When I look at the controls language by the letter, WAA and sWAA are scoped to personalization. I see no statement being made about collection for conversion tracking/measurement, which I believe means that it might still be allowed even under sWAA opt out.” Wu clarified that collection of users’ web and app activity data continues regardless of WAA/sWAA status. “When the user opt-out data collection control like WAA or YT history pause, the policy is not that we cannot collect data, but that the data we collected need to be deleted (or disconnected with the user identifier) within 63 days. In turns of how the data can be used, it also depends on the usage. e.g., For ads personalization, it’s not allowed. For measurement like conversion tracking, it’s generally allowed.”⁴²⁷

382. The WAA/sWAA user interface does not disclose that users’ web and app activity will continue to be collected—for conversion tracking and other undisclosed purposes—even if they have toggled the WAA/sWAA switch to “off.” It also does not disclose that Google will continue to save app activity data alongside persistent, Google-created and -controlled identifiers like AdID.

11.6. Google’s Disclosures to App Developers Exemplify Dark Patterns

383. Google has stated that the company “requires app developers to obtain consent from their users for the use of GA for Firebase.”⁴²⁸ For support, Google relies on the Google Analytics for Firebase Terms of Service⁴²⁹ and the Google Analytics for Firebase Use Policy.⁴³⁰ I have reviewed all versions of these documents in effect during the class period.

384. All four versions of the Google Analytics for Firebase Terms of Service affirm that Google will abide by the terms of its privacy policy: “Google and its Affiliates may retain and use, subject to the terms of its privacy policy (located at www.google.com/privacy.html), information collected in Your use of the Service.” All three versions of the Firebase Analytics Use Policy require developers to disclose “[h]ow App Users can opt-out of the Firebase

⁴²⁷ GOOG-RDGZ-00209109 at -12-14.

⁴²⁸ Google’s Second Supplemental Response to Interrogatory No. 7.

⁴²⁹ Google’s Second Supplemental Response to Interrogatory No. 7 lists the various versions of the Google Analytics for Firebase Terms of Service by Bates number—GOOG-RDGZ-00000905 (effective May 18, 2016); GOOG-RDGZ-00000902 (effective May 17, 2017); GOOG-RDGZ-00000916 (effective October 1, 2018); GOOG-RDGZ-00000910 (effective April 17, 2019). These produced versions consist of a single page, and are incomplete. I have therefore referred to the versions archived online: Google, “Archive: Firebase Analytics Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics/20160518> (May 18, 2016); Google, “Google Analytics for Firebase Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics/20170517> (May 17, 2017); Google, “Google Analytics for Firebase Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics/20181001> (October 1, 2018); Google, “Google Analytics for Firebase Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics> (April 17, 2019).

⁴³⁰ GOOG-RDGZ-00000914 (effective May 18, 2016); GOOG-RDGZ-00000908 (effective May 17, 2017); GOOG-RDGZ-00000900 (effective December 20, 2019).

Rodriguez v. Google

Analytics features you use, including through applicable device settings, such as the device advertising settings for mobile apps, or any other available means.”

385. These documents exemplify the dark pattern of “sneaking” because Google never informs app developers that data collection via Google services (like Google Analytics for Firebase) will override the privacy controls (like WAA) that Google offers users.

386. To the contrary, Google directs app developers to a user-facing page where Google reiterates its promise to users that they can control what data Google collects, including users’ activity on non-Google apps. The Google Analytics Terms of Service⁴³¹ and the Google Analytics for Firebase Terms of Service⁴³² recommends that app developers include in their own privacy policies a link to “How Google uses data when you use our partners’ sites or apps” (<http://www.google.com/policies/privacy/partners>).⁴³³ The subsection of “How Google Uses Information from Sites or Apps that Use Our Services” titled “How you can control the information collected by Google on these sites and apps” informs readers that they can use “My Activity...to review and control data that’s created when you use Google services, including the information we collect from the sites and apps you have visited.” The text contains a hyperlink to the “My Activity” page, where users can toggle WAA on or off.

387. Website publishers and app developers are also told that Google respects end users’ choices. The Analytics help page, “Safeguarding your data,” affirms the company’s “commitment to protecting the confidentiality and security of data,” and links to the Google Privacy Policy.⁴³⁴ Website publishers and app developers are told that the policy “describes how we treat personal information when you use Google’s products and services, including Google Analytics,” and details the methods by which end users may “adjust [their] privacy settings to control what we collect and how [their] information is used.”

388. In this way, Google’s behaviors toward app developers also exhibit the dark pattern of Aesthetic Manipulation. App developers are encouraged to believe that Google is providing controls for its own users to opt out of data collection, even in the context of Google’s collection of data relating to users’ activity on non-Google apps.

⁴³¹ Google, Google Analytics Terms of Service,” *Google Marketing Platform*, <https://marketingplatform.google.com/about/analytics/terms/us/> (last modified June 17, 2019).

⁴³² Google, “Google Analytics for Firebase Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics> (last modified April 17, 2019).

⁴³³ Google’s Second Supplemental Responses to Interrogatories No. 5, 6 and 8 list five versions of “How Google Uses Information from Sites or Apps that Use Our Services” by Bates number: GOOG-RDGZ-00020554 (April 20, 2018); GOOG-RDGZ-00020556 (May 11, 2018); GOOG-RDGZ-00020558 (April 24, 2020); GOOG-RDGZ-00020560 (April 24, 2020); GOOG-RDGZ-00020562 (May 26, 2020). Elsewhere, in its Responses to Interrogatories 6, 7 and 8, Google states that these documents have “production errors.” I am therefore commenting on the current version available online: Google, “How Google uses information from sites or apps that use our services,” *Google Privacy and Terms*, <https://policies.google.com/technologies/partner-sites> (accessed February 7, 2023). In its Responses to Interrogatory Nos. 6 and 7, Google provided an additional list by Bates number of 36 different versions of “How Google Uses Information from Sites or Apps that Use Our Services.” 21 of these documents consist of a single blank page; one consists of a single, unintelligible line; the rest appear to be excerpts. I have not relied upon these.

⁴³⁴ Google, “Safeguarding your data,” *Firebase Help*, <https://support.google.com/firebase/answer/6004245> (accessed January 26, 2023).

Rodriguez v. Google

11.7. Google Employees Repeatedly Identified Problems with Google’s Disclosures Regarding WAA/sWAA, but Google Ignored Them

389. I am not alone in identifying problems with Google’s disclosures about WAA and sWAA. The evidence in this case suggests that Google employees agree with me.

390. Google staff have recognized that the situation with respect to user control is far from transparent. In a 2018 internal document, David Monsees described the “opportunity” for improvement of Google’s existing user data controls (UDC): “UDC’s value prop [proposition] is not clear, what is the overall purpose of the settings. WAA and sWAA are too big and non-specific for users to understand; what is ‘web & app’.... UDC covers a lot, but only controls a fraction of the information that Google uses to personalize.”⁴³⁵

391. In a 2018 email thread, Dave Kleidermacher—now Google’s Vice President of Engineering for Android—wrote, “If a user could flip the switch at the device (or account) level and have confidence in not having activity tracked in ANY app, it would completely change the way privacy-conscious users and influencers view Google (and Android).”⁴³⁶ However, when asked in October 2022 whether such a switch had ever been implemented, Eric Miraglia replied that he was “not aware of any setting that’s scoped” that way.⁴³⁷

392. In a July 2019 email exchange with David Monsees, Chris Ruemmler expressed his continued concern that the WAA Help page “actually doesn’t describe what happens when the bit is disabled.”

“[I]t appears we have a real problem here with accurately describing what happens when WAA is disabled. We should fix the current wording to reflect reality and if we make the change to temp GAIA logging, then we need to be very clear about what data is collected with WAA off. [...] [G]iven the way on/off works, one has to then assume that disabled (off) would be the exact opposite of what is described for what happens when the WAA bit is on. Today, we don’t accurately describe what happens when WAA is off.... If I choose not to store data in my account, then Google should not have access to the data either as the data should not be in the account. What you are stating is WAA (or any of the other controls) does not actually control what is stored by Google, but simply what the user has access to. This is really bad. If we are storing data that the user does not have access to, we need to be clear about that fact. In this case, the user has a false sense of security that their data is not being stored at Google, when in fact it is.”⁴³⁸

393. Mr. Ruemmler reiterated his concerns in several 2020 email exchanges with colleagues: “Web and App Activity is the worst name ever. This is part of the problem with the WAA bit. What does it ACTUALLY control? It is not obvious at all from our documentation. We need to be very clear about what is controlled by this flag.”⁴³⁹ “I’m looking for something that explicitly

⁴³⁵ GOOG-RDGZ-00018270.

⁴³⁶ GOOG-RDGZ-00150939.

⁴³⁷ Miraglia Tr. 129:21-25; 130:2-3.

⁴³⁸ GOOG-RDGZ-00024709-10.

⁴³⁹ GOOG-RDGZ-00089546.

Rodriguez v. Google

describes all of the knobs and their default states. I don't think I could describe what exactly is enabled and disabled by WAA/SAA/etc. based on current documentation.”⁴⁴⁰ WAA, Mr. Ruemmler asserted, was “completely broken” with “no way for the user to determine what this actually controls.”⁴⁴¹

394. But in his deposition, Mr. Monsees acknowledged that no further action was taken to address Mr. Ruemmler's concerns, nor were any responsive modifications made to Google's WAA and sWAA disclosures.⁴⁴²

395. The statement, “When Web & App Activity is on, Google saves [certain categories of] information” fails to clarify that while certain categories of information collected by Google may not be explicitly tied to the Google Account identifier of a user who has turned WAA off, Google nonetheless collects numerous data points about WAA-off users' activity that are transmitted by way of Google services like Google Analytics for Firebase, AdMob, and Ad Manager. The main difference between WAA-on and WAA-off appears to be the visibility of ongoing data collection to the user.

396. Mr. Ruemmler also expressed his concerns about the clarity of Google's disclosures about Google's “My Activity” page, and about the range of information—and misinformation—about users' doings online that are collected and stored:

“I've uncovered several problems with My Activity over the last few weeks and wonder what its actual purpose is within Google. I understand this is where search history for google.com is stored and it allows users to view and delete that history. That is great. Anything else beyond search data, is quite frankly confusing. For instance, I found that very detailed Google Pay data is being included in My Activity which was quite shocking to me. I would expect that data to stay in Google Pay and not have a copy in My Activity. I also found false “Ads” activity that was not only incorrect but not useful even if it had been correct.... I also turned off WAA and still received both of the above entries in My Activity. Based on the external documentation, it sounds like turning off WAA should result in an empty My Activity, but that is not the case. I'm OK with that, but it should be very clear that WAA is not associated with everything in My Activity and I don't believe that is the case today.... The whole WAA story is also quite confusing.”⁴⁴³

“My Activity is confusing at best for your average user.... The product is not cohesive and thus confusing.”⁴⁴⁴

⁴⁴⁰ GOOG-RDGZ-00130745 at -47.

⁴⁴¹ GOOG-RDGZ-00130745 at -46.

⁴⁴² Monsees Tr. 235:5-25, 236:1-5.

⁴⁴³ GOOG-RDGZ-00151565.

⁴⁴⁴ GOOG-RDGZ-00043816.

Rodriguez v. Google

397. Chris Ruemmler is far from the only Google employee who expressed concerns about Google's disclosures pertaining to WAA/sWAA.

- In a February 2019 email, Group Product Marketer Ruchi Bezoles wrote that “WAA isn’t understood either.”⁴⁴⁵
- In a February 2019 product design document, a Google developer described the business rationale for its decision to require users to enable WAA for personalization in apps that previously had not needed it: “The steering committee elected to turn off personalization for WAA-off users and coupling logging policy with personalization decisions, due to concerns over loss of data for analysis and high percentage of users with WAA-off at the time (30–40%). The resulting product behavior is very confusing to users, particularly the growing class concerned about privacy.”⁴⁴⁶
- In an April 2019 email, UX Researcher Brenda Chen described the “ongoing struggle that people don’t understand what Web & App Activity is.”⁴⁴⁷
- In her outline for a February 2020 presentation on user interface design and privacy, Senior UX Director Sarah Hammond offered WAA as an example of a control that’s “a tricky one to understand.”⁴⁴⁸
- In a July 14, 2020, email, Group Product Manager J.K. Kearns wrote an email stating that “To me, it feels like a fairly significant bug that a user can choose to turn off WAA, but then we still collect and use the data (even locally).”⁴⁴⁹
- In a July 2020 chat exchange discussing WAA and sWAA, Google Vice-President Meagan Pi remarked that “I think I barely understand what all of these mean and most users won’t have a clue.”⁴⁵⁰
- In an August 2020 email, Senior Financial Analyst Henry Wong noted that “users who have turned off WAA...have given us a clear signal that they do not want Google to know what they are searching for” and while “technically we don’t,” “it just feels like we are tracking them even though they told us not to.”⁴⁵¹
- In an October 2020 email, Product Manager Sam Heft-Luthy of Google’s Privacy and Data Protection Office noted that “we’re stretching ourselves thin, especially given that we are doing a lot to get users to understand a system that is just fundamentally difficult to get (WAA, GAP, etc.).”⁴⁵²
- In a chat exchange that same month, Principal Engineer Othar Hansson described his feelings about Google’s consent settings: “imagine how this looks to a normal user. I feel like I only understand it myself because I took AP Google History.”⁴⁵³

⁴⁴⁵ GOOG-RDGZ-00171164.

⁴⁴⁶ GOOG-RDGZ-00046758 at -09

⁴⁴⁷ GOOG-RDGZ-00087964.

⁴⁴⁸ GOOG-RDGZ-00203674 at -75.

⁴⁴⁹ GOOG-RDGZ-00044478 at -82.

⁴⁵⁰ GOOG-RDGZ-00169704.

⁴⁵¹ GOOG-RDGZ-00044356.

⁴⁵² GOOG-RDGZ-00129096 at -97.

⁴⁵³ GOOG-RDGZ-00159759.

Rodriguez v. Google

- Also in October 2020, UX Manager Kalle Buschmann remarked more generally that “It is not only our consent that is too convoluted, the underlying approach and systems to capturing and using data as well. We can’t fix the ‘surface’ experience without radically changing the machine. Only then humans (users or Googlers) will have a chance to understand it.... Our goal is to give people a good sense of where their data is used....”⁴⁵⁴
- Likewise, that same month, Senior Interaction Designer Elyse Bellamy stated that “from my perspective we don’t (as a company) have a very even approach to determining what we need to ask permission for, and what we don’t—also, how much contextual information is appropriate/necessary to get consent.”⁴⁵⁵ Elsewhere Ms. Bellamy noted, “Not only are the implications of WAA extremely broad and varied, but people use Google in such diverse ways—much of the language intended to be comprehensive feels vague and hard-to-parse for non-engineers/lawyers.”⁴⁵⁶

398. Google has also conducted “numerous” user studies that have concluded that “WAA just isn’t clear to users.”⁴⁵⁷ For example, one User Experience Research study included as a “key insight” that “WAA settings are hard to understand.”⁴⁵⁸ Additionally, an April 2020 study titled “Retention Controls Comprehension” found that “all participants expected turning WAA toggle off to stop saving their activity” and “all participants expected turning off toggle to stop their activity from being saved.”⁴⁵⁹ In a June 2020 research proposal, senior research manager Arne de Booij anticipated that “Most respondents will believe that turning off WAA will result in no data being collected from their activity and no personalisation in Google products and services.”⁴⁶⁰ In his deposition, Mr. de Booij acknowledged that the subject pool for a study of user understanding of Google’s user device controls, including the WAA/sWAA controls, was “not a general population representative sample,” but consisted entirely of German citizens with a specific interest in privacy. A series of one-on-one interviews with the research subjects yielded the recommendation, “Be more explicit of the effects of activation/deactivation. Use simple language.” This recommendation implies that even privacy-conscious individuals did not understand Google’s privacy disclosures, or “the effects of activation/deactivation” of user controls.⁴⁶¹

11.8. Google Uses Dark Patterns to Manipulate User Behavior to Its Own Benefit

399. In 2003, I coined the term “security theater” to describe many ineffective, inconvenient and potentially dangerous (think certain body scanners⁴⁶²) security measures instituted by the

⁴⁵⁴ GOOG-RDGZ-00129042-43.

⁴⁵⁵ GOOG-RDGZ-00129084.

⁴⁵⁶ GOOG-RDGZ-00203679 at -80.

⁴⁵⁷ GOOG-RDGZ-00090236 at -39.

⁴⁵⁸ GOOG-RDGZ-00151484 at line 38.

⁴⁵⁹ GOOG-RDGZ-00182573 at -81.

⁴⁶⁰ GOOG-RDGZ-00043294.R at -99.

⁴⁶¹ de Booij Tr. 80:09-96:22.

⁴⁶² EPIC, “EPIC v. Department of Homeland Security: Full body scanner radiation risks,” Electronic Privacy Information Center, <https://epic.org/documents/epic-v-department-of-homeland-security-full-body-scanner-radiation-risks> (accessed January 18, 2023).

Rodriguez v. Google

Transportation Security Administration and other government agencies in the wake of the September 11 attacks. (I discuss this topic at length in my book *Beyond Fear*.⁴⁶³) The phrase “privacy theater” has more recently emerged to describe actions by governments and corporations that seem to protect privacy, but in fact do no such thing.⁴⁶⁴

400. My extensive experience in the field of computer security and privacy, and the evidence presented in this case, leads me to conclude that Google’s effort to position the company as a champion of user privacy at the same time that it assiduously accumulates data about users’ online activity—even when they take up the company’s offer to turn off Google tracking—is a form of “privacy theater,” one that is more concerned with managing users’ impressions than with respecting their privacy intentions.

Respectfully submitted by,



/s/ Bruce Schneier

Date: February 20, 2023

⁴⁶³ Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, Springer, https://archive.org/details/beyondfearthinki00schn_0 (2003).

⁴⁶⁴ Rohit Khare, “Privacy theater: Why social networks only pretend to protect you,” *Tech Crunch*, <https://techcrunch.com/2009/12/27/privacy-theater/>; (December 28, 2009).

Christopher Soghoian, “An end to privacy theater: Exposing and discouraging corporate disclosure of user data to the government,” *Minnesota Journal of Law, Science and Technology*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1656494 (August 10, 2010).

Gilad Edelman, “Google and the age of privacy theater,” *Wired*, <https://www.wired.com/story/google-floc-age-privacy-theater/> (March 18, 2021).

Ari Ezra Waldman, “How Big Tech turns privacy laws into privacy theater,” *Slate*, <https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html> (December 2, 2021).

Expert Report of Bruce Schneier

February 20, 2023

Appendix 1

Documents Considered

Public Documents

Paywalled material is marked with an asterisk, with full text appended at the end of this document.

42 Matters, “Top 15 analytics SDKs used in Android apps,” <https://42matters.com/sdk-analysis/top-analytics-sdks> (last updated January 12, 2023).

42 Matters, “Top 20 ad network SDKs used in Android apps,” <https://42matters.com/sdk-analysis/top-ad-network-sdks> (last updated January 12, 2023).

Mark Ackerman, “Sales of public data to marketers can mean big \$\$ for governments,” CBS Denver, <https://denver.cbslocal.com/2013/08/26/sales-of-public-data-to-marketers-can-mean-big-for-governments> (August 26, 2013).

- * Efthimios Alepis and Constantinos Patsakis, “Session fingerprinting in Android via web-to-app intercommunication,” *Security and Communication Networks*, <https://dl.acm.org/doi/10.1155/2018/7352030> (2018).

- * Erin Allday, “Google worker arrested for cyberstalking,” *SFGate*, <https://www.sfgate.com/crime/article/Google-worker-arrested-for-cyberstalking-5848161.php> (October 25, 2014).

- * Julia Angwin, et al., “AT&T helped U.S. spy on internet on a vast scale,” *New York Times*, <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html> (August 16, 2015).

Ron Amadeo, “Google Workspace to strip privacy control from admins, re-enable tracking,” *Ars Technica*, <https://arstechnica.com/gadgets/2022/02/confusing-google-workspace-privacy-change-will-re-enable-tracking-for-users> (February 2, 2022).

S. Abhishek Anand, et al., “Motion sensor-based privacy attack on smartphones,” arXiv:1907.05972, arXiv.org, <https://arxiv.org/pdf/1907.05972.pdf> (October 19, 2020).

- * Michael Barbaro and Tom Zeller Jr., “A face is exposed for AOL Search No. 4417749,” *New York Times*, <http://www.nytimes.com/2006/08/09/technology/09aol.html> (August 9, 2006).

Katherine E. Boronow, et al., “Privacy risks of sharing data from environmental health studies,” *Environmental Health Perspectives* 128, no. 1, <https://ehp.niehs.nih.gov/doi/10.1289/EHP4817> (January 2020).

Nandita Bose, “Amazon’s surveillance can boost output and possibly limit unions: Study,” Reuters, <https://www.reuters.com/article/amazon-com-workers-surveillance/amazons-surveillance-can-boost-output-and-possibly-limit-unions-study-idUSKBN25S3F2> (September 15, 2020).

- * Joshua Bote, “Google workers are eavesdropping on your private conversations via its smart speakers,” *USA Today*, <https://www.usatoday.com/story/tech/2019/07/11/google-home-smart-speakers-employees-listen-conversations/1702205001> (July 11, 2019).

- * Tim Bradshaw and Patrick McGee, “Apple develops alternative to Google search,” *Financial Times*, <https://www.ft.com/content/fd311801-e863-41fe-82cf-3d98c4c47e26> (October 28, 2020).

Laura Brandimarte, Alessandro Acquisti and George Loewenstein, “Misplaced confidences: Privacy and the control paradox,” *Social Psychological and Personality Science* 4, no. 3, <https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf> (May 2013).

Harry Brignull, “Dark patterns: Deception vs. honesty in web design,” *A List Apart*, <https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design> (November 1, 2011).

Harry Brignull, “Dark patterns: Inside the interfaces designed to trick you,” *The Verge*, <http://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you> (August 29, 2013).

Harry Brignull, “Hall of shame,” *Deceptive Design*, <https://www.deceptive.design/hall-of-shame/all> (accessed December 20, 2022).

Sergey Brin and Lawrence Page, “The anatomy of a large-scale hypertextual web search engine,” *Computer Networks and ISDN Systems* 30, no. 1-7, <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/334.pdf> (April 1998).

California Constitution, “Article 1 Declaration of Rights,” California Legislative Information, https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS§ionNum=SECTION%201.&article=I (Article 1 adopted 1879; Sec. 1 added Nov. 5, 1974, by Proposition 7, Resolution Chapter 90, 1974).

Ryan Calo, “Digital market manipulation,” *George Washington Law Review* 82, no. 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703 (August 2014).

Peter Cao, “Google reportedly paying Apple \$9 billion to remain default search engine in Safari on iOS,” *9to5 Mac*, <https://9to5mac.com/2018/09/28/google-paying-apple-9-billion-default-search-engine> (September 28, 2018).

Capitalize My Title, “How many pages is 138,000 words?” <https://capitalizemytitle.com/page-count/138000-words> (accessed February 10, 2023).

- * Benjamin Carlson, “Quote of the day: Google CEO compares data across millennia,” *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/07/quote-of-the-day-google-ceo-compares-data-across-millennia/344989> (July 3, 2010).

Fred H. Cate, Peter Cullen, and Viktor Mayer-Schonberger, “Data protection principles for the 21st century: Revising the 1980 OECD Guidelines,” Oxford Internet Institute, University of Oxford, http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf (March 2014).

Rosalie Chan and Hugh Langley, “Hundreds of Google employees call on company to change sexual-misconduct policies that they say put the burden on survivors,” *Business Insider*, <https://www.businessinsider.com/google-employees-alphabet-union-petition-justice-for-jessica-misconduct-policies-2021-7> (July 21, 2021).

Adrian Chen, “GCreep: Google engineer stalked teens, spied on chats (Updated),” *Gawker*, <https://www.gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats> (September 14, 2010).

Elaine Christie, “Tracking the trackers 2020: Web tracking’s opaque business model of selling users,” *Ghostery Blog*, <https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users> (2020).

Thomas Claburn, “Google’s ‘privacy-first’ ad tech FLoC squawks when Chrome goes Incognito, says expert. Web giant disagrees,” *The Register*, https://www.theregister.com/2021/03/15/google_floc_chrome_incognito (March 15, 2021).

CNBC, “Google CEO Eric Schmidt on privacy,” <https://www.youtube.com/watch?v=A6e7wFDHzew> (December 8, 2009).

Colorado Legislature, “Senate Bill 21-90: Colorado Privacy Act,” https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf (enacted July 7, 2021)

Commission Nationale de l'Informatique et des Libertés, "Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation," <https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance> (January 6, 2022).

Commission Nationale de l'Informatique et des Libertés, "Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC," <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> (January 21, 2019).

Competition Commission of India, "CCI imposes a monetary penalty of Rs. 1337.76 crore on Google for anti-competitive practices in relation to Android mobile devices," <https://www.cci.gov.in/antitrust/press-release/details/261/0> (October 20, 2022).

Competition Commission of India, "Order under Section 27 of the Competition Act, 2002," In re Alphabet Inc., Google LLC, etc., <https://www.cci.gov.in/antitrust/orders/details/1072/0>.

Consumer Financial Protection Bureau, "CFPB charges TransUnion and senior executive John Danaher with violating law enforcement order," <https://www.consumerfinance.gov/about-us/newsroom/cfpb-charges-transunion-and-senior-executive-john-danaher-with-violating-law-enforcement-order> (April 12, 2022).

Cornell Legal information Institute, "2 CFR § 200.79—Personally Identifiable Information (PII)," <https://www.law.cornell.edu/cfr/text/2/200.79> (accessed March 2, 2022).

- * Rob Copeland and Sarah E. Needleman, "Google's 'Project Nightingale' triggers federal inquiry," *Wall Street Journal*, <https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867> (November 13, 2019).
- * Rob Copeland, "Google's 'Project Nightingale' gathers personal health data on millions of Americans," *Wall Street Journal*, <https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790> (November 11, 2019).
- * Rob Copeland, Dana Mattioli and Melanie Evans, "Inside Google's quest for millions of medical records," *Wall Street Journal*, <https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700> (January 11, 2020).

Council of Europe, "European Convention on Human Rights," https://www.echr.coe.int/Documents/Convention_ENG.pdf (1953) ("Everyone has the right to respect for his private and family life, his home and his correspondence").

Joseph Cox, "Leaked document says Google fired dozens of employees for data misuse," *VICE*, <https://www.vice.com/en/article/g5gk73/google-fired-dozens-for-data-misuse> (August 4, 2021).

Ry Crist, "Haier's new air conditioner is the first Apple-certified home appliance," *CNET*, <https://www.cnet.com/home/kitchen-and-household/haiers-new-air-conditioner-is-the-first-apple-certified-home-appliance> (January 8, 2014).

Chris Crum, "Google eyes mouse movement as possible search relevancy signal," *WebProNews*, <https://www.webpronews.com/google-eyes-mouse-movement-as-possible-search-relevancy-signal> (July 13, 2010).

C-SPAN, "LIVE: Google CEO Sundar Pichai testifies on data collection (C-SPAN)," *YouTube*, <https://www.youtube.com/watch?v=WfbTbPEEJxI> at 43:10 (December 11, 2018).

Bennett Cyphers, "Google is testing its controversial new ad targeting tech in millions of browsers. Here's what we know," Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2021/03/google-testing-its-controversial-new-ad-targeting-tech-millions-browsers-heres> (March 30, 2021).

Bennett Cyphers, “Google says it doesn’t ‘sell’ your data. Here’s how the company shares, monetizes, and exploits it,” Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and> (March 19, 2020).

Bennett Cyphers, “How to disable ad ID tracking on iOS and Android, and why you should do it now,” Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now> (May 11, 2022).

Datenschutzbehörde, “Information der Datenschutzbehörde zur Entscheidung über die Verwendung von Google Analytics,” Bekanntmachungen der Datenschutzbehörde, <https://www.dsb.gv.at/download-links/bekanntmachungen.html> (December 22, 2021).

Paresh Dave, “Google’s app network quietly becomes huge growth engine,” Reuters, <https://www.reuters.com/article/idUSKCN1FZ0F9> (February 15, 2018).

Emily DeCiccio, “Privacy laws need updating after Google deal with HCA Healthcare, medical ethics professor says,” CNBC, <https://www.cnbc.com/2021/05/26/privacy-laws-need-updating-after-google-deal-with-hca-healthcare-medical-ethics-professor-says.html> (May 26, 2021).

Geert de Lombaerde, “\$2B company buys local auto shopping data venture,” *Nashville Post*, https://www.nashvillepost.com/2b-company-buys-local-auto-shopping-data-venture/article_37f98c02-ed8e-5bba-b069-cb251e8eb11a.html (April 10, 2015).

Christian de Looper and Daniel Martin, “From Android 1.0 to Android 10, here’s how Google’s OS evolved over a decade,” *Digital Trends*, <https://www.digitaltrends.com/mobile/android-version-history> (March 30, 2021).

- * Yves-Alexandre de Montjoye, et al., “Unique in the shopping mall: On the re-identifiability of credit card metadata,” *Science* 347, no. 6221, <https://www.science.org/doi/full/10.1126/science.1256297> (January 30, 2015).

Linda Di Geronimo, et al., “UI dark patterns and where to find them: A study of mobile applications and user perception,” CHI ‘20, April 25–30, 2020, Honolulu, HI, USA, <https://dl.acm.org/doi/pdf/10.1145/3313831.3376600> (April 2020).

Pam Dixon, “Testimony of Pam Dixon, Executive Director, World Privacy Forum, before the U.S. Senate Committee on Commerce, Science, and Transportation: What information do data brokers have on consumers, and how do they use it?” World Privacy Forum, <https://www.govinfo.gov/content/pkg/CHRG-113shrg95838/pdf/CHRG-113shrg95838.pdf> (December 18, 2013).

- * Zak Doffman, “Ashley Madison hack returns to ‘haunt’ its victims: 32 million users now watch and wait,” *Forbes*, <https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait> (February 1, 2020).
- * Zak Doffman, “Google’s latest tracking nightmare for Chrome comes in two parts,” *Forbes*, <https://www.Forbes.com/sites/zakdoffman/2021/10/02/stop-using-google-chrome-on-windows-10-android-and-apple-iphones-ipads-and-macs/?sh=4fcde6092f30> (October 2, 2021).

Jillian D’Onofro, “Google is shutting down its Plus social network sooner than expected after discovering a second security bug,” CNBC, <https://www.cnbc.com/2018/12/10/google-shutting-down-social-network-sooner-because-of-new-security-bug.html> (December 10, 2018).

DuckDuckGo, “Measuring the ‘filter bubble’: How Google is influencing what you click,” *SpreadPrivacy: The Official DuckDuckGo Blog*, <https://spreadprivacy.com/google-filter-bubble-study> (December 4, 2018).

- * Charles Duhigg, “Bilking the elderly, with a corporate assist,” *New York Times*, <http://www.nytimes.com/2007/05/20/business/20tele.html> (May 20, 2007).
 - * William H. Dutton et al., “The Internet trust bubble: Global values, beliefs and practices,” *World Economic Forum*, http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf (May 2014).
- Elizabeth Dwoskin, Adam Entous and Craig Timberg, “Google uncovers Russian-bought ads on YouTube, Gmail and other platforms,” *Washington Post*, <https://www.washingtonpost.com/news/the-switch/wp/2017/10/09/google-uncovers-russian-bought-ads-on-youtube-gmail-and-other-platforms> (October 9, 2017).
- Peter Eckersley, “How unique is your web browser?” Proceedings of the 10th International Conference on Privacy Enhancing Technologies, Berlin, <https://coveryourtracks.eff.org/static/browser-uniqueness.pdf> (July 2010).
- * Gilad Edelman, “Google and the age of privacy theater,” *Wired*, <https://www.Wired.com/story/google-floc-age-privacy-theater> (March 18, 2021).
- Jim Edwards, “Apple has quietly started tracking iPhone users again, and it's tricky to opt out,” *Business Insider*, <https://www.businessinsider.com/ifa-apples-iphone-tracking-in-ios-6-2012-10> (October 11, 2012).
- Jim Edwards, “Google's new ‘Advertising ID’ is now live and tracking Android phones: This is what it looks like,” *Business Insider*, <https://www.businessinsider.com/googles-new-advertising-id-is-now-live-and-tracking-new-android-phonesthis-is-what-it-looks-like-2014-1> (January 27, 2014).
- Jennifer Elias, “Google’s \$310 million sexual harassment settlement aims to set new industry standards,” *CNBC*, <https://www.cnbc.com/2020/09/29/googles-310-million-sexual-misconduct-settlement-details.html> (September 29, 2020).
- Justin Elliott and Lucas Waldron, “Here’s how TurboTax just tricked you into paying to file your taxes,” *Pro Publica*, <https://www.propublica.org/article/turbotax-just-tricked-you-into-paying-to-file-your-taxes> (April 22, 2019).
- Steven Englehardt, et al., “Cookies that give you away: The surveillance implications of web tracking,” *WWW ‘15: Proceedings of the 24th International Conference on World Wide Web*, https://senglehardt.com/papers/www15_cookie_surveil.pdf (May 18, 2015).
- EPIC, “EPIC v. Department of Homeland Security: Full body scanner radiation risks,” Electronic Privacy Information Center, <https://epic.org/documents/epic-v-department-of-homeland-security-full-body-scanner-radiation-risks> (accessed January 18, 2023).
- Frank Esposito, “Cashless tolls: Welcome to the dark future,” *Rockland/Westchester Journal News*, <https://www.lohud.com/story/news/investigations/2018/04/11/cashless-tolls-dark-future/439131002> (April 11, 2018).
- European Commission, “Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google’s search engine,” https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581 (July 18, 2018).
- European Commission, “The Digital Services Act package,” <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (November 24, 2022).
- European Union, “Charter of Fundamental Rights of The European Union,” https://www.europarl.europa.eu/charter/pdf/text_en.pdf (2000).
- European Union, “General data protection regulation (GDPR),” <https://gdpr-info.eu> (April 27, 2016).

- * Melanie Evans, “Google strikes deal with hospital chain to develop healthcare algorithms,” *Wall Street Journal*, <https://www.wsj.com/articles/google-strikes-deal-with-hospital-chain-to-develop-healthcare-algorithms-11622030401> (May 26, 2021).
- Greg Fair, “Improving our privacy controls with a new Google dashboard,” *The Keyword*, Google, <https://www.blog.google/topics/safety-security/improving-our-privacy-controls-new-google-dashboard> (September 8, 2017).
- Trine Falbe, Kim Andersen and Martin Michael Frederiksen, *White Hat UX: The Next Generation in User Experience*, pej gruppens forlag, <https://www.smashingmagazine.com/printed-books/white-hat-ux> (April 10, 2017).
- Stephen Farrell and Hannes Tschofenig, “Pervasive monitoring is an attack,” *Best Current Practice* 188, Internet Engineering Task Force, (May 2014).
- Jim Finkle, “Massive data breach at Experian exposes personal data for 15 million T-Mobile customers,” *Huffington Post*/Reuters, https://www.huffpost.com/entry/experian-hacked-tmobile_n_560e0d30e4b0af3706e0481e (October 2, 2015).
- FindLaw, “Is there a ‘right to privacy’ amendment?” <https://www.findlaw.com/injury/torts-and-personal-injuries/is-there-a-right-to-privacy-amendment.html> (September 30, 2019).
- Kelsey Fogarty and Zachary McAuliffe, “Is Google tracking you? Here’s how to check and stop it,” *CNET*, <https://www.cnet.com/tech/services-and-software/is-google-tracking-you-heres-how-to-check-and-stop-it> (December 3, 2022).
- Tony Foley, “Google settles with state AGs over location-tracking,” *Cybersecurity Policy Report*, <https://www.vitallaw.com/news/cybersecurity-policy-report-google-settles-with-state-ags-over-location-tracking-nov-14-2022/cspd01c4651b62a7664db7a65684bef2600b6c> (November 14, 2022).
- Forbrukerrådet (Norwegian Consumer Council), “Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy,” <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> (June 27, 2018).
- * Geoffrey A. Fowler, “What does your car know about you? We hacked a Chevy to find out,” *Washington Post*, <https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out> (December 17, 2019).
- * Geoffrey Fowler, “87 percent of websites are tracking you,” *Washington Post*, <https://www.washingtonpost.com/technology/2020/09/25/privacy-check-blacklight> (September 25, 2020).
- Josh Fruhlinger, “Equifax data breach FAQ: What happened, who was affected, what was the impact?” *CSO Magazine*, <https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html> (February 12, 2020).
- * Barton Gellman and Laura Poitras, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program,” *Washington Post*, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-inbroad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (June 7, 2013).
- * Thomas Germain, “How a photo’s hidden ‘Exif’ data exposes your personal information,” *Consumer Reports*, <https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data-a2386546443> (December 6, 2019).

David Gilbert, “Companies turn to Switzerland for cloud storage following NSA spying revelations,” *International Business Times*, <http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613> (July 4, 2013).

- * Shane Goldmacher, “How Trump steered supporters into unwitting donations,” *New York Times*, <https://www.nytimes.com/2021/04/03/us/politics/trump-donations.html> (April 3, 2021).

Philippe Golle, “Revisiting the uniqueness of simple demographics in the U.S. population,” 5th ACM Workshop on Privacy in the Electronic Society (WPES’06), Alexandria, Virginia, <https://crypto.stanford.edu/~pgolle/papers/census.pdf> (October 30, 2006).

Google Workspace Team, “[Action Advised] Review new Workspace search history control for users [email],” <https://pastebin.com/raw/5ayJTDDp> (January 31, 2022).

Google Workspace, “Google Workspace (online) agreement,” https://workspace.google.com/terms/2013/1/premier_terms.html (October 6, 2020).

Google, “[GA4] Automatically collected events,” *Analytics Help*, https://support.google.com/analytics/answer/9234069?hl=en&ref_topic=9756175 (accessed December 21, 2022).

Google, “[GA4] Demographic details report,” *Analytics Help*, <https://support.google.com/analytics/answer/12948931> (accessed February 11, 2023).

Google, “[GA4] Enhanced event measurement,” *Analytics Help*, <https://support.google.com/analytics/answer/9216061> (accessed December 21, 2022).

Google, “[GA4] Predefined user dimensions,” *Analytics Help*, <https://support.google.com/firebase/answer/9268042> (accessed December 21, 2022).

Google, “About Google,” <https://about.google> (accessed February 20, 2023).

Google, “About keyword matching options,” *Search Ads 360 (new experience) Help*, <https://support.google.com/sa360/answer/9322510> (accessed January 13, 2023).

Google, “Activity controls,” *Google Account*, <https://myactivity.google.com/activitycontrols> (accessed January 31, 2023).

Google, “Automatically collected user properties,” *Google AdMob Help*, <https://support.google.com/admob/answer/9755590?hl=en> (accessed January 27, 2023).

Google, “Counting impressions and clicks,” *Google Ad Manager Help*, <https://support.google.com/admanager/answer/2521337?hl=en> (accessed February 11, 2023).

Google, “Find & control your Web & App Activity,” *Google Account Help*, <https://support.google.com/accounts/answer/54068> (accessed December 20, 2022).

Google, “Gmail,” *Apple App Store*, <https://apps.apple.com/us/app/gmail-email-by-google/id422689480> (accessed January 12, 2023).

Google, “Google Analytics for Firebase Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics> (last modified April 17, 2019).

Google, “Archive: Firebase Analytics Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics/20160518> (May 18, 2016).

Google, “Google Analytics for Firebase Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics/20170517> (May 17, 2017).

Google, “Google Analytics for Firebase Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics/20181001> (October 1, 2018).

Google, “Google Analytics for Firebase Terms of Service,” *Firebase Support*, <https://firebase.google.com/terms/analytics> (April 17, 2019).

Google, “Google Analytics Terms of Service,” *Google Marketing Platform*, <https://marketingplatform.google.com/about/analytics/terms/us/> (last modified June 17, 2019).

Google, “Google Chrome,” *Apple App Store*, <https://apps.apple.com/us/app/google-chrome/id535886823> (accessed February 20, 2023).

Google, “Google Classroom,” *Apple App Store*, <https://apps.apple.com/us/app/google-classroom/id924620788> (accessed January 12, 2023).

Google, “Google Drive,” *Apple App Store*, <https://apps.apple.com/us/app/google-drive/id507874739> (accessed January 12, 2023).

Google, “Google Home,” *Apple App Store*, <https://apps.apple.com/us/app/google-home/id680819774> (accessed January 12, 2023).

Google, “Google Maps,” *Apple App Store*, <https://apps.apple.com/us/app/google-maps/id585027354> (accessed January 12, 2023).

Google, “Google Meet,” *Apple App Store*, <https://apps.apple.com/us/app/google-meet/id1096918571> (accessed January 12, 2023).

Google, “Google Photos,” *Apple App Store*, <https://apps.apple.com/us/app/google-classroom/id924620788> (accessed January 12, 2023).

Google, “Google privacy policy: Sharing your information,” <https://policies.google.com/privacy?hl=en-US#infosharing> (February 10, 2022).

Google, “Mute ads on sites that partner with Google,” <https://support.google.com/authorizedbuyers/answer/2695260?hl=en> (accessed February 20, 2023).

Google, “My activity,” <https://myactivity.google.com> (first archived June 28, 2016).

Google, “Our privacy and security principles,” <https://safety.google/principles> (accessed December 23, 2022).

Google, “Overview of apps with Ad Manager,” *Google Ad Manager Help*, <https://support.google.com/admanager/answer/6238688?hl=en> (accessed February 11, 2023).

Google, “Privacy controls,” *Google Safety Center*, <https://safety.google/privacy/privacy-controls> (accessed January 31, 2023).

Google, “Privacy policy,” <https://policies.google.com/privacy> (effective December 15, 2022).

Google, “Real surveillance reform: What’s private is private, and the government should respect that,” <https://www.google.com/takeaction/issue/surveillance> (first archived October 3, 2015).

Google, “Safeguarding your data,” *Firebase Help*, <https://support.google.com/firebase/answer/6004245> (accessed January 26, 2023).

Google, “Takeout,” <https://takeout.google.com> (accessed February 20, 2023).

Google, “YouTube,” *Apple App Store*, <https://apps.apple.com/us/app/youtube-watch-listen-stream/id544007664> (accessed January 12, 2023).

Megan Graham and Jennifer Elias, “How Google’s \$150 billion advertising business works,” *CNBC*, <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html> (May 18, 2021).

Colin M. Gray, et al., “The dark (patterns) side of UX design,” *CHI 2018*, Montreal, Quebec, Canada, <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (April 21-26, 2018).

- * Jay Greene, “Amazon’s employee surveillance fuels unionization efforts: ‘It’s not prison, it’s work,’” *Washington Post*, <https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions> (December 2, 2021).
- * Jay Greene, “Tech giants have to hand over your data when federal investigators ask. Here’s why,” *Washington Post*, <https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation> (June 15, 2021).
- Seena Gressin, “The Marriott data breach,” U.S. Federal Trade Commission, <https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach> (December 4, 2018).
- * Alisha Haridasani Gupta and Natasha Singer, “Your app knows you got your period. Guess who it told?” *New York Times*, <https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html> (January 28, 2021).
- Hacker News, “Google to turn on activity tracking for many users who turned it off,” <https://news.ycombinator.com/item?id=30171800> (February 1, 2022).
- Jan Hannemann, “More transparency and control in your Google account,” *The Keyword*, Google, <https://blog.google/technology/safety-security/more-transparency-and-control-your-google-account> (June 21, 2018).
- * Amy Harmon, “As public records go online, some say they’re too public,” *New York Times*, <https://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html> (August 24, 2001).
- Michael X. Heiligenstein, “Google data breaches: Full timeline through 2022,” *Firewall Times*, <https://firewalltimes.com/google-data-breach-timeline> (January 18, 2022).
- Benjamin Henne, Maximilian Koch, and Matthew Smith, “On the awareness, control and privacy of shared photo metadata,” Distributed Computing & Security Group, Leibniz University, presented at the Eighteenth International Conference for Financial Cryptography and Data Security, Barbados, http://ifca.ai/fc14/papers/fc14_submission_117.pdf (March 3-7, 2014).
- * Alex Hern, “Facebook usage falling after privacy scandals, data suggests,” *The Guardian*, <https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows> (June 20, 2019).
- * Alex Hern, “Royal Free breached UK data law in 1.6m patient deal with Google’s DeepMind,” *The Guardian*, <https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act> (July 3, 2017).
- * Alex Hern, “Three quarters of Android apps track users with third party tools—study,” *The Guardian*, <https://www.theguardian.com/technology/2017/nov/28/android-apps-third-party-tracker-google-privacy-security-yale-university> (November 28, 2017).
- Hannah Hewitt, “The Austrian Data Protection Authority ground-breaking Google Analytics decision: Analysis and key takeaways,” Orrick Herrington & Sutcliffe LLP, <https://www.orrick.com/en/Insights/2022/02/The-Austrian-Data-Protection-Authority-Groundbreaking-Google-Analytics-Decision> (February 2, 2022).
- * Kashmir Hill, “I tried to live without the tech giants. It was impossible,” *New York Times*, <https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html> (July 31, 2020).
- Hitachi Data Systems, “The internet on wheels and Hitachi, Ltd.,” <https://docplayer.net/2138869-The-internet-on-wheels-and-hitachi-ltd-by-hitachi-data-systems.html> (November 2014).
- William Hoffman, et al., “Rethinking personal data: Trust and context in user-centred data ecosystems,” World Economic Forum,

http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (May 2014).

Aaron Holmes, “533 million Facebook users’ phone numbers and personal data have been leaked online,” *Business Insider*, <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4> (April 3, 2021).

Chris Jay Hoofnagle, “The Potemkinism of privacy pragmatism,” *Slate*, http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.html (September 2, 2014).

Jingyu Hua, Zhenyu Shen and Sheng Zhong, “We can track you if you take the metro: Tracking metro riders using accelerometers on smartphones,” arXiv:1505.05958, arXiv.org, <https://arxiv.org/abs/1505.05958v1> (May 22, 2015).

Matthew Humphries, “Mozilla signs lucrative 3-year Google search deal for Firefox,” *PC Magazine*, <https://www.pcmag.com/news/mozilla-signs-lucrative-3-year-google-search-deal-for-firefox> (August 14, 2020).

Alison Hung, “Keeping consumers in the dark: Addressing ‘nagging’ concerns and injury,” *Columbia Law Review* 121, <https://columbialawreview.org/content/keeping-consumers-in-the-dark-addressing-nagging-concerns-and-injury> (2021).

IAB Europe, “The EU’s proposed new cookie rules 1: digital advertising, European media, and consumer access to online news, other content and services,” <https://brave.com/static-assets/files/1b-IAB-2017-paper.pdf> (November 20, 2018).

Greg Iacurci, “TurboTax owner Intuit to pay \$141 million to customers ‘unfairly charged,’” CNBC, <https://www.cnbc.com/2022/05/04/turbotax-owner-intuit-to-pay-141-million-to-customers.html> (May 4, 2022).

S&P Global, “S&P Global, now part of S&P Global acquired business asserts of Dataium,” <https://spglobal.com/en/enterprise/btp/dataium.html> (accessed February 20, 2023).

Scott Ikeda, “Google and Facebook hit with fines over dark patterns allegedly misleading users into cookie consent,” *CPO Magazine*, <https://www.cpomagazine.com/data-protection/google-and-facebook-hit-with-fines-over-dark-patterns-allegedly-misleading-users-into-cookie-consent> (January 11, 2022).

ITC Secure, “Firebase Cloud Messaging vulnerability potentially affecting billions,” ITC Secure, <https://itcsecure.com/threat-horizon/firebase-cloud-messaging-vulnerability-potentially-affecting-billions> (August 28, 2020).

Chris Jackson and Catherine Morris, “Americans report high levels of concern about data privacy and security,” Ipsos, <https://www.ipsos.com/en-us/americans-report-high-levels-concern-about-data-privacy-and-security> (March 16, 2021).

Artur Janc and Lukasz Olejnik, “Web browser history detection as a real-world privacy threat,” *ESORICS’10: Proceedings of the 15th European Conference on Research in Computer Security*, <http://cds.cern.ch/record/1293097/files/LHCb-PROC-2010-036.pdf> (September 20, 2010).

Andrea Jelinek, et al., “Dark patterns in social media platform interfaces: How to recognise and avoid them,” Version 1.0, European Data Protection Board, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (14 March 2022).

Maitrik Kataria, “App usage statistics 2022 that’ll surprise you (updated),” Simform, <https://www.simform.com/blog/the-state-of-mobile-app-usage> (January 5, 2021; last updated November 11, 2022).

Michael Kassner, “Anatomy of the Target data breach,” *ZD Net*, <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned> (February 2, 2015).

Graham Kates, “Facebook, for the first time, acknowledges election manipulation,” CBS News, <https://www.cbsnews.com/news/facebook-for-the-first-time-acknowledges-election-manipulation> (April 28, 2017).

Rohit Khare, “Privacy theater: Why social networks only pretend to protect you,” *TechCrunch*, <https://techcrunch.com/2009/12/27/privacy-theater/>; (December 28, 2009).

Guemmy Kim, “Celebrating My Account’s first birthday with improvements and new controls,” *The Keyword*, Google, <https://blog.google/technology/safety-security/celebrating-my-accounts-first-birthday> (June 1, 2016).

Guemmy Kim, “Keeping your personal information private and safe—and putting you in control,” *The Keyword*, Google, <https://blog.google/topics/safety-security/privacy-security-tools-improvements> (June 1, 2015).

- * Jason Kint, “The Russia ad story isn’t just about Facebook. It’s about Google, too,” *Washington Post*, https://www.washingtonpost.com/opinions/the-russia-ad-story-isnt-just-about-facebook-its-about-google-too/2017/10/31/061055da-be5d-11e7-8444-a0d4f04b89eb_story.html (October 31, 2017).

- * Jemima Kiss, “Google admits collecting Wi-Fi data through Street View cars,” *The Guardian*, <https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data> (May 15, 2010).

Knopf Doubleday Publishing Group, “Google executives to publish new book with Knopf,” <http://knopfdoubleday.com/2012/12/03/google-executives-to-publish-new-book-with-knopf> (December 3, 2012).

- * John Koetsier, “Google is tracking you on 86% of the top 50,000 websites on the planet,” *Forbes*, <https://www.forbes.com/sites/johnkoetsier/2020/03/11/google-is-tracking-you-on-86-of-the-top-50000-websites-on-the-planet> (March 11, 2020).

Dániel Kondor, et al., “Towards matching user mobility traces in large-scale datasets,” arXiv:1709.05772, <https://arxiv.org/pdf/1709.05772.pdf> (August 13, 2018).

Brian Krebs, “Experian API exposed credit scores of most Americans,” *Krebs on Security*, <https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans> (April 28, 2021).

Selena Larson, “Every single Yahoo account was hacked—3 billion in all,” *CNN Business*, <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html> (October 4, 2017).

Joseph J. Lazzarotti and Mary T. Costigan, “CCPA FAQs on cookies,” *National Law Review* 13, no. 52, <https://www.natlawreview.com/article/ccpa-faqs-cookies> (August 29, 2019).

Dave LeClair, “Mozilla says Chrome’s latest feature enables surveillance,” *How-To Geek*, <https://www.howtogeek.com/756338/mozilla-says-chromes-latest-feature-enables-surveillance> (September 21, 2021).

Douglas J. Leith, “Mobile handset privacy: Measuring the data iOS and Android send to Apple and Google,” International Conference on Security and Privacy in Communication Systems (SecureComm) 2021: Security and Privacy in Communication Networks, https://www.scss.tcd.ie/doug.leith/apple_google.pdf (March 25, 2021).

Douglas J. Leith, “Web browser privacy: What do browsers say when they phone home?” *IEEE Access* 9, https://www.scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf (March 19, 2021).

Adam Lerner, et al., “Internet Jones and the Raiders of the Lost Trackers: An archaeological study of web tracking from 1996 to 2016,” 15th USENIX Security Symposium, August 10-12, 2016, Austin, TX, <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner> (2016).

- * Cristiano Lima and Aaron Schaffer, “Google is manipulating browser extensions to stifle competitors, DuckDuckGo CEO says,” *Washington Post*, <https://www.washingtonpost.com/politics/2022/01/05/google-is-manipulating-browser-extensions-stifle-competitors-duckduckgo-ceo-says/> (January 5, 2022).

Johnny Lin and Sean Halloran, “Study: Effectiveness of Apple's App Tracking Transparency,” *Transparency Matters*, <https://blog.lockdownprivacy.com/2021/09/22/study-effectiveness-of-apples-app-tracking-transparency.html> (September 22, 2021).

Litmus, “Email client market share in April 2022,” <https://www.litmus.com/blog/email-client-market-share-april-2022> (April 2022).

Natasha Lomas, “France fines Google \$120M and Amazon 42M for dropping tracking cookies without consent,” *Tech Crunch*, <https://techcrunch.com/2020/12/10/france-fines-google-120m-and-amazon-42m-for-dropping-tracking-cookies-without-consent/> (December 10, 2020).

Natasha Lomas, “Google confirms it’s pulling the plug on Streams, its UK clinician support app,” *Tech Crunch*, <https://techcrunch.com/2021/08/26/google-confirms-its-pulling-the-plug-on-streams-its-uk-clinician-support-app/> (August 26, 2021).

Natasha Lomas, “Google fails to overturn EUJ’s €4BN+ Android antitrust decision,” *Tech Crunch*, <https://techcrunch.com/2022/09/14/google-eu-android-antitrust-appeal-ruling/> (September 14, 2022).

Ben Lovejoy, “Google paid Apple almost \$10 billion in 2018, ‘Apple Prime’ service needed in 2019 says Goldman Sachs,” *9to5 Mac*, <https://9to5mac.com/2019/02/12/google-paid-apple-prime-service/> (February 12, 2019).

Gila Lyons, “An ode to Two Dots, the game that eases my anxious mind,” *VICE*, https://www.vice.com/en_us/article/zmkdea/two-dots-iphone-game-anxiety-stress-relief-sleep (September 5, 2018).

- * Douglas MacMillan and Robert McMillan, “Google exposed user data, feared repercussions of disclosing to public,” *Wall Street Journal*, <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194> (October 8, 2018).
- * Wayne Madsen, “The Clipper controversy,” *Information Systems Security* 3, <http://www.sciencedirect.com/science/article/pii/S1353485894900973> (November 1994).

Johnny Makes, “Why Google’s new search results design is a dark pattern,” *UX Design*, <https://uxdesign.cc/why-googles-new-search-results-design-is-a-dark-pattern-168935802f95> (January 23, 2020).

Angelica Mari, “Experian challenged over massive data leak in Brazil,” *ZD Net*, <https://www.zdnet.com/article/experian-challenged-over-massive-data-leak-in-brazil/> (February 20, 2021).

David Martin, “Dark patterns: Impact on consumers and potential harm,” Public Hearing, Committee on the Internal Market and Consumer Protection, <https://www.europarl.europa.eu/cmsdata/246802/BEUC%20PPT%20Dark%20Patterns%20Hearing%20IMCO-16%20March%202022.pdf> (March 16, 2022).

Jonathan Mayer, Patrick Mutchler and John C. Mitchell, “Evaluating the privacy properties of telephone metadata,” *Proceedings of the National Academy of Sciences* 113, no. 20, <http://www.pnas.org/cgi/doi/10.1073/pnas.1508081113> (May 17, 2016).

Justin McCarthy, “One in five U.S. adults use health apps, wearable trackers,” Gallup, <https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx> (December 11, 2019).

McKinsey & Company, “What’s driving the connected car,” <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car> (September 1, 2014).

Ellen Messmer, “NSA scandal spooking IT pros in UK, Canada,” *Network World*, <http://www.networkworld.com/article/2173190/security/nsa-scandal-spooking-it-pros-in-uk-canada.html> (January 8, 2014).

Meta Platforms, Inc., “Form 10-K,” United States Securities and Exchange Commission, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/e574646c-c642-42d9-9229-3892b13aabfb.pdf> (February 3, 2023).

Mighty Signal, “Firebase Android SDK,” <https://mightysignal.com/sdk/android/1432/firebase> (accessed December 2, 2022).

Chance Miller, “Analysts: Google to pay Apple \$15 billion to remain default Safari search engine in 2021,” *9to5Mac*, <https://9to5mac.com/2021/08/25/analysts-google-to-pay-apple-15-billion-to-remain-default-safari-search-engine-in-2021> (August 25, 2021).

Minima, “Firebase billing surprises: How to really cap your spending,” <https://blog.minimacode.com/cap-firebase-spending> (January 28, 2022).

Eric Miraglia, “Privacy that works for everyone,” *The Keyword*, Google, <https://blog.google/technology/safety-security/privacy-everyone-io> (May 7, 2019).

Dennis Moons, “Dark patterns in Google Ads,” *Store Growers*, <https://www.storegrowers.com/dark-patterns-google-ads> (December 12, 2022).

Phil Muncaster, “Experian data breach hits 24 million customers,” *InfoSecurity Magazine*, <https://infosecurity-magazine.com/news/experian-data-breach-24-million> (August 20, 2020).

- * Craig Mundie, “Privacy pragmatism: Focus on data use, not data collection,” *Foreign Affairs* 93, <http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism> (March/April 2014).

Ryan Nakashima, “Google clarifies location-tracking policy,” Associated Press, <https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211> (August 16, 2018).

Ryan Nakashima, “Google tracks your movements, like it or not,” Associated Press, <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb> (August 13, 2018).

Arvind Narayanan and Vitaly Shmatikov, “Robust de-anonymization of large sparse datasets,” 2008 IEEE Symposium on Security and Privacy, Oakland, California, <https://web.stanford.edu/class/cs245/win2020/readings/netflix-deanonymization.pdf> (May 18-20, 2008).

Arvind Narayanan, et al., “Dark patterns: Past, present and future,” *ACM Queue* 18, no. 2, <https://queue.acm.org/detail.cfm?id=3400901&doi=10.1145%2F3400899.3400901> (May 17, 2020).

National Institute of Standards and Technology, Computer Security Resource Center, “Glossary,” <https://csrc.nist.gov/glossary/term/privacy> (accessed February 20, 2023).

Nerdwriter, “How dark patterns trick you online,” *YouTube*, <https://youtu.be/kxkrdLI6e6M> (March 28, 2018).

Nest, “Nest Learning Thermostat,”

<https://files.bbystatic.com/vhTV4lnOCsNyVEpOkxhbpQ%3D%3D/0541791a-0142-49e2-a7ca-2bf505340b4d.pdf> (2018).

Nest, “Nest Protect (Wired 120V ~ 60Hz) user’s guide,” [https://nest.com/support/images/misc-assets/Nest-Protect-\(Wired-120V\)-User-s-Guide.pdf](https://nest.com/support/images/misc-assets/Nest-Protect-(Wired-120V)-User-s-Guide.pdf) (June 17, 2014).

Sean O’Brien and Michael Kwet, “#BlackFriday announcement from Privacy LAB,” *Information Society Project*, Yale Law School, <https://privacylab.yale.edu/trackers.html> (November 24, 2017).

Office of the Attorney General, “Attorney General James secures \$2.6 million from online travel agency for deceptive marketing,” <https://ag.ny.gov/press-release/2022/attorney-general-james-secures-26-million-online-travel-agency-deceptive> (March 16, 2022).

Office of the Attorney General, “California Consumer Privacy Act,” <https://oag.ca.gov/privacy/ccpa> (accessed February 20, 2023).

Paul Ohm, “Broken promises of privacy: Responding to the surprising failure of anonymization,” *UCLA Law Review* 57, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (August 13, 2009).

Lukasz Olejnik, Claude Castelluccia and Artur Janc, “Why Johnny can’t browse in peace: On the uniqueness of web browsing history patterns,” *Annals of Telecommunications* 1-2, <https://hal.inria.fr/file/index/docid/747841/filename/johnny2hotpet-finalcam.pdf> (June 2013).

Opera Limited, “Opera and Google renew search agreement,” *PR Newswire*, <https://www.prnewswire.com/news-releases/opera-and-google-renew-search-agreement-301448072.html> (December 20, 2021).

ORCHA, “Data privacy matters...Period: Data security of period tracking apps,” Organization for the Review of Care and Health Apps, <https://info.orchhealth.com/data-security-period-tracking-apps> (August 9, 2022).

Organization for Economic Cooperation and Development, “The OECD privacy framework,” http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (2013).

Elsie Otachi, “How to delete an Amazon account,” *Help Desk Geek*, <https://helpdeskgeek.com/how-to/how-to-delete-an-amazon-account> (August 11, 2020).

* Oxford English Dictionary Online, “Mute” (retrieved March 7, 2022).

* Oxford English Dictionary Online, “Private” (retrieved February 28, 2022).

Larry Page and Charlie Rose, “Where’s Google going next?” TED, https://www.ted.com/talks/larry_page_where_s_google_going_next?language=en (March 2014).

Jose Pagliery, “5 million Gmail passwords leaked,” *CNN Business*, <https://money.cnn.com/2014/09/10/technology/security/gmail-hack/index.html> (September 10, 2014).

Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin (2011).

Matti Pärssinen, et al., “Environmental impact assessment of online advertising,” *Environmental Impact Assessment Review* 73, <https://www.sciencedirect.com/science/article/pii/S0195925517303505#!> (November 2018).

Frank Pasquale, “The troubling trend toward trade secret-protected ranking systems,” Chicago Intellectual Property Colloquium, Chicago, Illinois, <http://www.chicagoip.com/pasquale.pdf> (April 21, 2009).

Joshua M. Pearce, “Energy conservation with open source ad blockers,” *Technologies* 8, no. 18, <https://www.mdpi.com/2227-7080/8/2/18/htm> (March 30, 2020).

Angela Cordoba Perez and Jose R. Gonzalez, “Arizona announces \$85M settlement with Google for allegedly tracking users’ location deceptively,” *Arizona Republic*, <https://www.azcentral.com/story/news/local/arizona-breaking/2022/10/04/mark-brnovich-announces-85-m-settlement-google-after-investigation/8176001001> (October 4, 2022).

Sarah Perez and Zack Whittaker, “Period tracker Stardust surges following Roe reversal, but its privacy claims aren’t airtight,” *Tech Crunch*, <https://techcrunch.com/2022/06/27/stardust-period-tracker-phone-number> (June 27, 2022).

Sarah Perez, “Google’s CEO thinks Android users know how much their phones are tracking them,” *Tech Crunch*, <https://techcrunch.com/2018/12/11/google-ceo-sundar-pichai-thinks-android-users-know-how-much-their-phones-are-tracking-them> (December 11, 2018).

Pew Research Center, “Internet/broadband fact sheet,” <https://www.pewresearch.org/internet/fact-sheet/internet-broadband> (April 7, 2021).

- * Sundar Pichai, “Google’s Sundar Pichai: Privacy should not be a luxury good,” *New York Times*, <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html> (May 7, 2019).

Jon Porter, “Brave browser replaces Google with its own search engine,” *The Verge*, <https://www.theverge.com/2021/10/20/22736142/brave-browser-search-engine-default-google-quant-duckduckgo-web-discovery-project> (October 20, 2021).

- * Kevin Poulsen and Robert McMillan, “TikTok tracked user data using tactic banned by Google,” *Wall Street Journal*, <https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738> (August 11, 2020).

Meg Prater, “25 Google search statistics to bookmark ASAP,” *HubSpot*, <https://blog.hubspot.com/marketing/google-search-statistics> (June 9, 2021).

President’s Council of Advisors on Science and Technology, “Big data and privacy: A technology perspective,” http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (May 2014).

PrivacyTools.io, “Exodus for Android: Finds trackers embedded in all your apps,” <https://www.privacytools.io/guides/exodus-for-android-finds-trackers> (page accessed December 7, 2022).

ProPublica, “The TurboTax trap (Series index),” <https://www.propublica.org/series/the-turbotax-trap> (accessed February 20, 2023).

- * Mizanur Rahman, et al., “Towards de-anonymization of Google Play search rank fraud,” *IEEE Transactions on Knowledge and Data Engineering* 33, no. 11, <https://ieeexplore.ieee.org/document/9003210> (November 2021).

Joel Reardon, et al., “50 ways to leak your data: An exploration of apps’ circumvention of the Android permissions system,” PrivacyCon 2019, Washington, D.C., https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serger_egelman.pdf (June 27, 2019).

- * Catherine Roberts, “Period tracker apps and privacy,” *Consumer Reports*, <https://www.consumerreports.org/health-privacy/period-tracker-apps-privacy-a2278134145> (May 25, 2022).
- Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de *oye, “Estimating the success of re-identifications in incomplete datasets using generative models,” *Nature Communications* 10, article 3069, <https://www.nature.com/articles/s41467-019-10933-3> (July 23, 2019).
- Salvador Rodriguez, “Some advertisers are quitting Facebook, chiding the company’s ‘despicable business model’,” CNBC, <https://www.cnbc.com/2019/03/06/some-advertisers-are-quitting-facebook-after-privacy-scandals.html> (March 6, 2019).
- Joe Rossignol, “Apple reportedly storing over 8 million terabytes of iCloud data on Google servers,” *MacRumors*, <https://www.macrumors.com/2021/06/29/icloud-data-stored-on-google-cloud-increasing> (June 29, 2021).
- Rahul Roy-Chowdhury, “Data Privacy Day: Seven ways we protect your privacy,” *The Keyword*, Google, <https://blog.google/technology/safety-security/data-privacy-day-seven-ways-we-protect-your-privacy> (January 28, 2020).
- Ethan Russell, “9 things to know about Google’s maps data: Beyond the map,” *Google Cloud Blog*, <https://cloud.google.com/blog/products/maps-platform/9-things-know-about-googles-maps-data-beyond-map> (September 30, 2019).
- Johnny Ryan, “The biggest data breach,” Irish Council for Civil Liberties, <https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf> (May 16, 2022).
- Ajavi Abimbola Samuel, “Top 10 big companies using Firebase,” *Career Karma*, <https://careerkarma.com/blog/companies-that-use-firebase> (February 10, 2022).
- * Adam Satariano and Jack Nicas, “E.U. fines Google \$5.1 billion in Android antitrust case,” *New York Times*, <https://www.nytimes.com/2018/07/18/technology/google-eu-android-fine.html> (July 18, 2018).
- * Eric Savitz, “Apple should buy a search engine, analyst says,” *Barron’s*, <https://www.barrons.com/articles/amazon-stock-split-51646863502> (June 8, 2020).
- Douglas C. Schmidt, et al., “Google data collection,” Vanderbilt University, <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf> (August 15, 2018).
- Eric Schmidt and Jared Cohen, *The New Digital Age*, Knopf, https://archive.org/details/newdigitalageres0000schm_w0t9 (2013).
- Caroline Schneider and Clément Le Biez, “Media websites: 70% of the carbon footprint caused by ads and stats,” Marmelab, <https://marmelab.com/blog/2022/01/17/media-websites-carbon-emissions.html> (January 17, 2022).
- Bruce Schneier, *A Hacker’s Mind: How the Powerful Bend Society’s Rules, and How to Bend them Back*, WW Norton & Co, 2023.
- Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, <https://archive.org/details/appliedcryptogra0000schn> (1994).
- Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, Springer, https://archive.org/details/beyondfearthinki0000schn_0 (2003).
- Bruce Schneier, *Data and Goliath*, Norton, <https://archive.org/details/datagoliathhidde0000schn> (2015).

Justin Schuh, “Building a more private web,” *The Keyword*, Google, <https://www.blog.google/products/chrome/building-a-more-private-web> (August 27, 2019).

Mathew J. Schwartz, “Google Aurora hack was Chinese counterespionage operation,” *Dark Reading*, <https://www.darkreading.com/attacks-breaches/google-aurora-hack-was-chinese-counterespionage-operation> (May 21, 2013).

Stephen Shankland, “Sundar Pichai: Chrome ‘exceptionally profitable’ for Google (q&a),” *CNET*, <https://www.cnet.com/tech/services-and-software/sundar-pichai-chrome-exceptionally-profitable-for-google-q-a> (June 29, 2012).

Seed Scientific, “How much data is created every day?” <https://seedscientific.com/how-much-data-is-created-every-day> (October 28, 2021).

Harvey Silverglate, *Three Felonies a Day: How the Feds Target the Innocent*, Encounter Books, <https://archive.org/details/harveya.silverglatethreefeloniesadayhowthefedstargettheinnocentencounterbooks20092> (2011).

* Natasha Singer, “Acxiom lets consumers see data it collects,” *New York Times*, <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html> (September 5, 2013).

* Natasha Singer, “Acxiom, the quiet giant of consumer database marketing: Mapping, and sharing, the consumer genome,” *New York Times*, <https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html> (June 16, 2012).

* Jeremy Singer-Vine, “How Dataium watches you,” *Wall Street Journal*, <http://blogs.wsj.com/digits/2012/12/07/howdataium-watches-you> (December 7, 2012).

Manish Singh, “India fines Google \$162 million for anti-competitive practices on Android,” *Tech Crunch*, <https://techcrunch.com/2022/10/20/india-fines-google-162-million-for-anti-competitive-practices-on-android> (October 20, 2022).

Antoinette Siu, “TikTok can circumvent Apple and Google privacy protections and access full user data, 2 studies say (Exclusive),” *Yahoo! News*, <https://www.yahoo.com/entertainment/tiktok-circumvent-apple-google-privacy-140000271.html> (February 14, 2022).

Christopher Soghoian, “An end to privacy theater: Exposing and discouraging corporate disclosure of user data to the government,” *Minnesota Journal of Law, Science and Technology*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1656494 (August 10, 2010).

Hyojin Song and Simon Wilkie, “The price of privacy in the cloud: The economic consequences of Mr. Snowden.” Microsoft Corporation. https://dornsife.usc.edu/assets/sites/586/docs/song_wilkie_2017.pdf (February 2017).

Statcounter, “Desktop search engine market share worldwide,” <https://gs.statcounter.com/search-engine-market-share/desktop/worldwide> (accessed December 21, 2022).

Statcounter, “Mobile operating system market share United States of America, Nov 2021—Nov 2022,” <https://gs.statcounter.com/os-market-share/mobile/united-states-of-america> (accessed December 28, 2022).

Statcounter, “Mobile operating system market share worldwide, Nov 2021—Nov 2022,” <https://gs.statcounter.com/os-market-share/mobile/worldwide> (accessed December 28, 2022).

Statcounter, “Mobile search engine market share worldwide, November 2021-November 2022,” <https://gs.statcounter.com/search-engine-market-share/mobile/worldwide> (accessed December 21, 2022).

Surfshark, “Uncovering the apps that actually respect your privacy,” <https://surfshark.com/apps-that-track-you> (May 14, 2021).

Latanya Sweeney, “Only you, your doctor, and many others may know,” *Technology Science* 2018, <https://techscience.org/a/2015092903> (September 28, 2015).

Latanya Sweeney, “Simple demographics often identify people uniquely,” Carnegie Mellon University Data Privacy Working Paper 3, <https://dataprivacylab.org/projects/identifiability/paper1.pdf> (2000).

- * Latanya Sweeney, “Weaving technology and policy together to maintain confidentiality,” *Journal of Law, Medicine and Ethics* 25, <http://onlinelibrary.wiley.com/doi/10.1111/j.1748-720X.1997.tb01885.x/abstract> (June 1997).

Latanya Sweeney, Akua Abu and Julia Winn, “Identifying participants in the Personal Genome Project by name (A re-identification experiment),” [arxiv.org, https://arxiv.org/abs/1304.7605](https://arxiv.org/abs/1304.7605) (2013).

James Tamplin, “Firebase is joining Google!” *The Firebase Blog*, <https://firebase.blog/posts/2014/10/firebase-is-joining-google> (October 21, 2014).

Rosie Taylor, “Popular period-tracking apps are sharing sensitive personal data with advertisers including cycle dates, contraception use and how often you’re having sex, study reveals,” *Daily Mail*, <https://www.dailymail.co.uk/sciencetech/article-11045653/Popular-period-tracking-apps-sharing-sensitive-personal-data-advertisers-study-finds.html> (July 25, 2022).

Tech Shielder, “Hacker hotspots: The apps most vulnerable to cybercrime,” <https://techshielder.com/hacker-hotspots-most-vulnerable-apps> (September 2, 2022).

David Thacker, “Expediting changes to Google+,” *The Keyword*, Google, <https://www.blog.google/technology/safety-security/expediting-changes-google-plus> (December 10, 2018).

David Temkin, “Google charts a course towards a more privacy-first web,” Google Ads and Commerce Blog, <https://blog.google/products/ads-commerce/a-more-privacy-first-web> (March 3, 2021).

- * Derek Thompson, “Google’s CEO: ‘The laws are written by lobbyists’,” *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/#video> (October 1, 2010).
- * Craig Timberg, “Brokers use ‘billions’ of data points to profile Americans,” *Washington Post*, https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html (May 27, 2014).
- * Ariana Tobin, Justin Elliott and Meg Marco, “Here are your stories of being tricked into paying by TurboTax. You often need the money,” ProPublica, <https://www.propublica.org/article/here-are-your-stories-of-being-tricked-into-paying-by-turbotax-you-often-need-the-money> (April 26, 2019).

Christof Ferreira Torres and Hugo Jonker, “Investigating fingerprinters and fingerprinting-alike behaviour of Android applications,” *European Symposium on Research in Computer Security (ESORICS 2018) Proceedings*, Springer-Verlag, https://link.springer.com/chapter/10.1007/978-3-319-98989-1_4 (August 7, 2018).

Roman Unuchek, “Leaking ads: Is user data truly secure?” RSA 2018, San Francisco, <https://published-prd.lanyonevents.com/published/rsaus18/sessionsFiles/8161/ASEC-T08-Leaking-Ads-Is-User-Data-Truly-Secure.pdf> (April 16-20, 2018).

- * Bruce Upbin, “The web is much bigger (and smaller) than you think,” *Forbes*, <https://www.forbes.com/sites/ciocentral/2012/04/24/the-web-is-much-bigger-and-smaller-than-you-think> (April 24, 2012).
- U.S. Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> (November 2021).
- U.S. Department of Energy, “The smart grid: An introduction,” [http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages\(1\).pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf) (2008).
- U.S. Executive Office of the President, “Big data: Seizing opportunities, preserving values,” http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (May 1, 2014).
- U.S. Federal Bureau of Investigation, “Chinese military hackers charged in Equifax breach,” <https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020> (February 10, 2020).
- U.S. Federal Trade Commission, “Developer of popular women’s fertility-tracking app settles FTC allegations that it misled consumers about the disclosure of their health data,” <https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about> (January 13, 2021).
- U.S. Federal Trade Commission, “Bringing dark patterns to light,” Staff Report, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (September 2022).
- U.S. Federal Trade Commission, “Complaint,” FTC v. Lending Club Corporation, Case 3:18-cv-02454, https://www.ftc.gov/system/files/documents/cases/lending_club_complaint.pdf (filed April 25, 2018).
- U.S. Federal Trade Commission, “Fortnite video game maker Epic Games to pay more than half a billion dollars over FTC allegations of privacy violations and unwanted charges,” <https://www.ftc.gov/news-events/news/press-releases/2022/12/fornite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations> (December 19, 2022).
- U.S. Federal Trade Commission, “FTC action against Vonage results in \$100 million to customers trapped by illegal dark patterns and junk fees when trying to cancel service,” <https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-action-against-vonage-results-100-million-customers-trapped-illegal-dark-patterns-junk-fees-when-trying-cancel-service> (November 3, 2022).
- U.S. Federal Trade Commission, “FTC sues Intuit for its deceptive TurboTax “free” filing campaign,” <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-sues-intuit-its-deceptive-turbotax-free-filing-campaign> (March 29, 2022).
- U.S. Federal Trade Commission, “FTC takes action to stop Credit Karma from tricking consumers with allegedly false ‘pre-approved’ credit offers,” <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-takes-action-stop-credit-karma-tricking-consumers-allegedly-false-pre-approved-credit-offers> (September 1, 2022).
- U.S. Federal Trade Commission, “Google and YouTube will pay record \$170 million for alleged violations of children’s privacy law,” <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> (September 4, 2019).

U.S. Federal Trade Commission, “Google to refund consumers at least \$19 million to settle FTC complaint it unlawfully billed parents for children’s unauthorized in-app charges,” <https://www.ftc.gov/news-events/news/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it-unlawfully-billed-parents-childrens> (September 4, 2014).

U.S. Federal Trade Commission, “Google will pay \$22.5 million to settle FTC charges it misrepresented privacy assurances to users of Apple’s Safari internet browser,” <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> (August 9, 2012).

U.S. Federal Trade Commission, “LendingClub agrees to pay \$18 million to settle FTC charges,” <https://www.ftc.gov/news-events/news/press-releases/2021/07/lendingclub-agrees-pay-18-million-settle-ftc-charges> (July 24, 2021).

U.S. Federal Trade Commission, “Notice of settlement with state Attorneys General,” In the matter of Intuit Inc., Federal Trade Commission Office of Administrative Law Judges Docket No. 94-9, https://www.ftc.gov/system/files/ftc_gov/pdf/D09408%20-%20NOTICE%20OF%20SETTLEMENT%20WITH%20STATE%20ATTORNEYS%20GENERAL%20-%20PUBLIC%20%281%29.pdf (May 5, 2022).

U.S. Federal Trade Commission, “Rent-to-own payment plan company Progressive Leasing will pay \$175 million to settle FTC charges it deceived consumers about pricing,” <https://www.ftc.gov/news-events/news/press-releases/2020/04/rent-own-payment-plan-company-progressive-leasing-will-pay-175-million-settle-ftc-charges-it> (April 20, 2020).

U.S. House of Representatives, “Written testimony of Sundar Pichai, Chief Executive Officer, Alphabet, Inc.,” Online platforms and market power, part 6: Examining the dominance of Amazon, Apple, Facebook, and Google,” Hearing Before the Subcommittee on Antitrust, Commercial, and Administrative Law of the House Committee on the Judiciary, <https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-PichaiS-20200729.pdf> (July 29, 2020).

U.S. Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, “A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes,” Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

U.S. Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, “A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes,” Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

U.S. Supreme Court, “Decision,” United States v. Jones, Case No. 10-1259, <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=000&invol=10-1259#opinion1> (January 23, 2012).

United Nations Office of the High Commissioner for Human Rights, “The right to privacy in the digital age,” <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx> (2021).

United Nations, “Universal Declaration of Human Rights,” <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (December 10, 1948) (“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence”).

- * Jennifer Valentino-DeVries and Jeremy Singer-Vine, “They know what you’re shopping for,” *Wall Street Journal*, <http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214> (December 7, 2012).

Brandon Vigliarolo, “Marriott Hotels admits to third data breach in 4 years,” *The Register*, https://www.theregister.com/2022/07/06/marriott_hotels_suffer_yet_another (July 6, 2022).

Antonio Villas-Boas, “Passwords are incredibly insecure, so websites and apps are quietly tracking your mouse movements and smartphone swipes without you knowing to make sure it’s really you,” *Business Insider*, <https://www.businessinsider.com/websites-apps-track-mouse-movements-screen-swipes-security-behavioral-biometrics-2019-7> (July 19, 2019).

Paul Vines, Franziska Roesner and Tadayoshi Kohno, “Exploring ADINT: Using ad targeting for surveillance on a budget, or How Alice can buy ads to track Bob,” ACM Workshop on Privacy in the Electronic Society, WPES '17, Dallas, Texas, <https://dl.acm.org/doi/pdf/10.1145/3139550.3139567> (October 30, 2017).

Christian M. Wade, “Cashless tolls on Mass. Pike raise revenue, privacy concerns,” *Salem News*, https://www.salemnews.com/news/state_news/cashless-tolls-on-mass-pike-raise-revenue-privacy-concerns/article_325861fa-079c-5a82-b155-0a7339e2af6e.html (September 22, 2016).

- * Daisuke Wakabayashi, “Google will no longer scan Gmail for ad targeting,” *New York Times*, <https://www.nytimes.com/2017/06/23/technology/gmail-ads.html> (June 23, 2017).
- * Daisuke Wakabayashi, “Google’s shadow work force: Temps who outnumber full-time employees,” *New York Times*, <https://www.nytimes.com/2019/05/28/technology/google-temp-workers.html> (May 28, 2019).
- * Daisuke Wakabayashi, Kate Conger and Brian X. Chen, “Google introduces a new system for tracking Chrome browser users,” *New York Times*, <https://www.nytimes.com/2022/01/25/business/google-topics-chrome-tracking.html> (January 25, 2022).

Ari Ezra Waldman, “How Big Tech turns privacy laws into privacy theater,” *Slate*, <https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html> (December 2, 2021).

Stephen T. Walker, “Oral testimony by Stephen T. Walker, President, Trusted Information Systems, Inc., for Subcommittee on Economic Policy, Trade and Environment, Committee on Foreign Affairs, U.S. House of Representatives,” https://irp.fas.org/congress/1993_hr/931012_walker_oral.htm (October 12, 1993).

Mark R. Warner, “Lawmakers announce additional support for bipartisan, bicameral legislation to ban manipulative ‘dark patterns,’” Office of Mark R. Warner, <https://www.warner.senate.gov/public/index.cfm/2022/6/lawmakers-announce-additional-support-for-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns> (June 15, 2022).

Mark R. Warner, “Lawmakers reintroduce bipartisan bicameral legislation to ban manipulative ‘dark patterns,’” Office of Mark R. Warner, <https://www.warner.senate.gov/public/index.cfm/2021/12/lawmakers-reintroduce-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns> (December 8, 2021).

Mark R. Warner, “Senators introduce bipartisan legislation to ban manipulative ‘dark patterns,’” Office of Mark R. Warner, <https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns> (April 9, 2019).

- * Charlie Warzel, “The loophole that turns your apps into spies,” *New York Times*, <https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html> (September 24, 2019).

Peter Watts, “The scorched earth society,” Symposium of the International Association of Privacy Professionals, Toronto, Ontario, <https://rifiers.com/real/shorts/TheScorchedEarthSociety-transcript.pdf> (May 9, 2014).

Alma Whitten, “Updating our privacy policies and terms of service,” *Google Official Blog*, <https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html> (January 24, 2012).

Wikipedia, “Automated readability index,” https://en.wikipedia.org/wiki/Automated_readability_index (accessed February 20, 2023).

Wikipedia, “Coleman-Liau index,” https://en.wikipedia.org/wiki/Coleman%E2%80%93Liau_index (February 20, 2023).

Wikipedia, “Flesch-Kincaid readability tests,” https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests (accessed February 20, 2023).

Wikipedia, “Flesch-Kincaid readability tests,” https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests (accessed February 20, 2023).

Wikipedia, “Gunning fog index,” https://en.wikipedia.org/wiki/Gunning_fog_index (accessed February 20, 2023).

Wikipedia, “Lexical density,” https://en.wikipedia.org/wiki/Lexical_density (accessed February 20, 2023).

Wikipedia, “SMOG,” <https://en.wikipedia.org/wiki/SMOG> (accessed February 20, 2023).

Ben Wojdyla, “How it works: The computer inside your car,” *Popular Mechanics*, <http://www.popularmechanics.com/cars/how-to/repair/how-it-works-the-computer-inside-your-car> (February 21, 2012).

Simon Wright, “Autonomous cars generate more than 300 TB of data per year,” Tuxera, <https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year> (July 2, 2021).

- * Eli Jacobson, et al., “De-identification is insufficient to protect student privacy, or What can a field trip reveal?” *Journal of Learning Analytics* 8, no 2, <https://www.learning-analytics.info/index.php/JLA/article/view/7353> (2021).

Ji Su Yoo, et al., “Risks to patient privacy: A re-identification of patients in Maine and Vermont statewide hospital data,” *Technology Science* 2018, <https://techscience.org/a/2018100901> (October 8, 2018).

- * Cat Zakrzewski, Pranshu Verma and Claire Parker, “Texts, web searches about abortion have been used to prosecute women,” *Washington Post*, <https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution> (July 3, 2022).

Paul A. Zandbergen and Sean J. Barbeau, “Positional accuracy of assisted GPS data from high-sensitivity GPS-enabled mobile phones,” *Journal of Navigation* 64, http://www.paulzandbergen.com/files/Zandbergen_Barbeau_JON_2011.pdf (July 2011).

Paul A. Zandbergen, “Accuracy of iPhone locations: A comparison of assisted GPS, WiFi and cellular positioning,” *Transactions in GIS* 13, https://www.paulzandbergen.com/PUBLICATIONS_files/Zandbergen_TGIS_2009.pdf (June 26, 2009).

Maciej Zawadzinski, “The case against Google Analytics for organizations collecting personal data,” *CPO Magazine*, <https://www.cpomagazine.com/data-privacy/the-case-against-google-analytics-for-organizations-collecting-personal-data> (September 1, 2020).

David Zetoony, Christian Auty and Karin Ross, “Answers to the most frequently asked questions concerning cookies and adtech,” Bryan Cave Leighton Paisner, <https://ccpa-info.com/wp-content/uploads/2019/08/Handbook-of-FAQs-Cookies.pdf> (February 2020).

- * Kim Zetter, “Google hackers targeted source code of more than 30 companies,” *Wired*, <https://www.wired.com/2010/01/google-hack-attack> (January 13, 2010).

Shoshana Zuboff, *The Age of Surveillance Capitalism*, New York: Public Affairs, <https://archive.org/details/shoshanazubofftheageofsurveillancecapitalism> (2019).

Deposition Transcripts

2022-02-17 Deposition Transcript of Sal Cataldo
 2022-03-07 Deposition Transcript of Julian Santiago
 2022-08-09 Deposition Transcript of Ethan Dunn
 2022-09-09 Deposition Transcript of Christopher Ruemmler
 2022-09-15 Deposition Transcript of David Monsees
 2022-09-23 Deposition Transcript of Edward Weng
 2022-10-03 Deposition Transcript of Greg Fair
 2022-10-16 Deposition Transcript of Anibal Rodriquez
 2022-10-25 Deposition Transcript of Eric Miraglia
 2022-10-27 Deposition Transcript of Susan Harvey
 2022-10-28 Deposition Transcript of Francis Ma
 2022-10-28 Deposition Transcript of Steve Ganem
 2022-11-15 Deposition Transcript of Daniel Stone
 2022-11-18 Deposition Transcript of Rahul Oak
 2022-12-15 Deposition Transcript of Belinda Langner
 2023-02-07 Deposition Transcript of Arne De Booij
 2023-02-08 Rough Deposition Transcript of Sam Heft-Luthy
 2023-02-09 Rough Deposition Transcript of Xinyu Ye

Case Filings and Orders

2020-01-11 Rodriguez v Google- Dkt 60 Pltfs First Amended Complaint
 2020-10-13 Rodriguez v Google- Dkt 48 Def Google’s Motion to Dismiss
 2020-12-17 Rodriguez v Google- Dkt 62 Def Google’s Motion to Dismiss
 2021-05-21 Rodriguez v Google- Dkt 109 Order on Motion to Dismiss
 2021-09-20 Rodriguez v Google- Dkt 138 Pltfs Third Amended Complaint
 2022-01-25 Rodriguez v Google- Dkt 209 Order Granting Motion to Dismiss
 2023-01-04 Rodriguez v. Google- Dkt 289 Pltfs Fourth Amended Complaint
 2023-02-03 Rodriguez v. Google- Dkt 305 Def Google’s Answer to Complaint

Other Case Filings

2020-05-21 Arizona v Google- Complaint
2022-05-04 Arizona v Google- Expert Report of Colin M. Gray, Ph.D.
2022-06-08 Arizona v Google- Expert Rebuttal Report of Donna L. Hoffman, Ph.D
2021-11-30 Calhoun v Google- Def Google's Motion for Summary Judgment
2021-11-30 Calhoun v Google- Fair Declaration ISO Def Google's Motion for Summary Judgment

Written Discovery

2020-11-25 Rodriguez v Google- Def Google's Responses to Plaintiffs' Request for Admissions Set One
2021-02-26 Rodriguez v Google- Def Google's Supplemental Responses to Plaintiffs' Interrogatories, Set One
2022-07-13 Rodriguez v Google- Def Google's Responses to Plaintiffs' Interrogatories Set Six
2022-10-11 Rodriguez v Google- Def Google's Responses to Request for Admissions Set Three
2022-10-26 Rodriguez v Google- Def Google's Supplemental Response to Interrogatory 15
2022-10-31 Rodriguez v Google- Def Google's Responses to Interrogatories Set Seven
2022-10-31 Rodriguez v Google- Def Google's Second Supplemental Responses to Interrogatories Nos. 6-8
2022-10-31 Rodriguez v Google- Def Google's Supplemental Response to Interrogatory Nos. 12, 16, 17
2022-11-07 Rodriguez v Google- Def Google's Supplemental Responses to Request for Admissions Set 4

Produced Documents

GOOG-RDGZ-00000400
GOOG-RDGZ-00000410
GOOG-RDGZ-00000417
GOOG-RDGZ-00000434
GOOG-RDGZ-00000451
GOOG-RDGZ-00000468
GOOG-RDGZ-00000485
GOOG-RDGZ-00000502
GOOG-RDGZ-00000519
GOOG-RDGZ-00000529
GOOG-RDGZ-00000557
GOOG-RDGZ-00000585
GOOG-RDGZ-00000613
GOOG-RDGZ-00000642
GOOG-RDGZ-00000672
GOOG-RDGZ-00000703
GOOG-RDGZ-00000735

GOOG-RDGZ-00000900
GOOG-RDGZ-00000902
GOOG-RDGZ-00000905
GOOG-RDGZ-00000908
GOOG-RDGZ-00000910
GOOG-RDGZ-00000914
GOOG-RDGZ-00000916
GOOG-RDGZ-00000923
GOOG-RDGZ-00000929
GOOG-RDGZ-00000935
GOOG-RDGZ-00013515
GOOG-RDGZ-00013851
GOOG-RDGZ-00014421
GOOG-RDGZ-00014556
GOOG-RDGZ-00014578
GOOG-RDGZ-00015004
GOOG-RDGZ-00015764
GOOG-RDGZ-00018270
GOOG-RDGZ-00018996
GOOG-RDGZ-00020299
GOOG-RDGZ-00020554
GOOG-RDGZ-00020556
GOOG-RDGZ-00020558
GOOG-RDGZ-00020560
GOOG-RDGZ-00020740
GOOG-RDGZ-00024123
GOOG-RDGZ-00024709
GOOG-RDGZ-00025713
GOOG-RDGZ-00025811
GOOG-RDGZ-00031656
GOOG-RDGZ-00033244
GOOG-RDGZ-00033245
GOOG-RDGZ-00037515
GOOG-RDGZ-00039094
GOOG-RDGZ-00041092
GOOG-RDGZ-00043294.R
GOOG-RDGZ-00043816
GOOG-RDGZ-00044356
GOOG-RDGZ-00044478
GOOG-RDGZ-00046758
GOOG-RDGZ-00046758.R
GOOG-RDGZ-00046896
GOOG-RDGZ-00047446
GOOG-RDGZ-00052671
GOOG-RDGZ-00053380
GOOG-RDGZ-00056142

GOOG-RDGZ-00059283
GOOG-RDGZ-00059486
GOOG-RDGZ-00061316
GOOG-RDGZ-00061878
GOOG-RDGZ-00070506
GOOG-RDGZ-00087672
GOOG-RDGZ-00087672
GOOG-RDGZ-00087914
GOOG-RDGZ-00087964
GOOG-RDGZ-00089546
GOOG-RDGZ-00090067
GOOG-RDGZ-00090236
GOOG-RDGZ-00090741
GOOG-RDGZ-00100625
GOOG-RDGZ-00116371
GOOG-RDGZ-00117318
GOOG-RDGZ-00118026
GOOG-RDGZ-00126932
GOOG-RDGZ-00128059
GOOG-RDGZ-00128280
GOOG-RDGZ-00128911
GOOG-RDGZ-00129042
GOOG-RDGZ-00129084
GOOG-RDGZ-00129096
GOOG-RDGZ-00130322
GOOG-RDGZ-00130381
GOOG-RDGZ-00130745
GOOG-RDGZ-00131231
GOOG-RDGZ-00131856
GOOG-RDGZ-00139579
GOOG-RDGZ-00145259, cited in Miraglia Tr. 55:10-12
GOOG-RDGZ-00146347
GOOG-RDGZ-00149527
GOOG-RDGZ-00149701
GOOG-RDGZ-00149771
GOOG-RDGZ-00150067
GOOG-RDGZ-00150939
GOOG-RDGZ-00151484
GOOG-RDGZ-00151565
GOOG-RDGZ-00151568
GOOG-RDGZ-00152809
GOOG-RDGZ-00154623
GOOG-RDGZ-00156520
GOOG-RDGZ-00159759
GOOG-RDGZ-00160654
GOOG-RDGZ-00164257

GOOG-RDGZ-00164312
GOOG-RDGZ-00168139
GOOG-RDGZ-00169704
GOOG-RDGZ-00171164
GOOG-RDGZ-00173562
GOOG-RDGZ-00180854
GOOG-RDGZ-00181801
GOOG-RDGZ-00182573
GOOG-RDGZ-00184222
GOOG-RDGZ-00184248
GOOG-RDGZ-00184488
GOOG-RDGZ-00185669
GOOG-RDGZ-00188602
GOOG-RDGZ-00188616
GOOG-RDGZ-00188632
GOOG-RDGZ-00188868
GOOG-RDGZ-00203345
GOOG-RDGZ-00203387
GOOG-RDGZ-00203545
GOOG-RDGZ-00203674
GOOG-RDGZ-00203679
GOOG-RDGZ-00206996
GOOG-RDGZ-00207105
GOOG-RDGZ-00208190

Expert Report of Bruce Schneier

February 20, 2023

Appendix 2 Curriculum Vitae

Bruce Schneier

Contact: schneier@schneier.com

Background

Bruce Schneier is an internationally renowned security technologist, called a “security guru” by the *Economist*. He is the *New York Times* best-selling author of 14 books—including *Click Here to Kill Everybody*—as well as hundreds of articles, essays, and academic papers. His influential newsletter *Crypto-Gram* and blog *Schneier on Security* are read by over 250,000 people. Schneier is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of EPIC and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.

Professional Experience

2019–present, Chief of Security Architecture, Inrupt, Inc., Boston, MA.

2016–2019, Chief Technology Officer, IBM Resilient, and special advisor to IBM Security, Cambridge, MA.

2014–2016, Chief Technology Officer, Resilient Systems, Inc. (formerly called Co3 Systems, Inc.), Cambridge, MA.

2006–2013, Chief Security Technology Officer, British Telecom, London, UK.

1999–2006, Chief Technology Officer, Counterpane Internet Security, Inc., Cupertino, CA.

1993–1999, President, Counterpane Systems, Oak Park, IL and Minneapolis, MN.

1991–1993, Member of Technical Staff, AT&T Bell Labs., Schaumburg, IL.

1990, Director of Operations, Intelligent Resources Information Systems, Inc., Chicago, IL.

1987–1990, Program Manager, Space and Naval Warfare Systems Command, Arlington, VA.

1984–1987, Electronics Engineer, Naval Electronics Systems Security Engineering Center, Washington, DC.

Academic Experience

2016+, Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University.

2016–2018, Research Fellow in the Science, Technology, and Public Policy program at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

2013+, Fellow, Berkman Klein Center for Internet and Society, Harvard University.

Board Membership

2017+, Board Member, AccessNow, New York, NY

2013+, Board Member, Electronic Frontier Foundation, San Francisco, CA.

2016–2021, Board Member, Tor Project, Cambridge, MA.

2004–2013, Board Member, Electronic Privacy Information Center, Washington DC.

Education

MS Computer Science, American University, 1986.

BS Physics, University of Rochester, 1984.

Books

A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back, WW Norton & Co., 2022.

We Have Root: Even More Advice from Schneier on Security, John Wiley & Sons, 2019.

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, WW Norton & Co., 2018.

Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World, WW Norton & Co., 2015.

Carry On: Sound Advice from Schneier on Security, John Wiley & Sons, 2013.

Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons, 2012.

Bruce Schneier CV: Academic Publications**3**

Cryptography Engineering (with Niels Ferguson and Tadayoshi Kohno), John Wiley & Sons, 2010.

Schneier on Security, John Wiley & Sons, 2008.

Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Copernicus Books, 2003.

Practical Cryptography (with Niels Ferguson), John Wiley & Sons, 2003

Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, 2000.

The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance (with David Banisar), John Wiley & Sons, 1997.

Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

The Twofish Encryption Algorithm (with John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson), John Wiley & Sons, 1996.

E-Mail Security, John Wiley & Sons, 1995

Protect Your Macintosh, Peachpit Press, 1994

Applied Cryptography, John Wiley & Sons, 1994.

Academic Publications

J. Penney and B. Schneier, “Platforms, Encryption, and the CFAA: The Case of *WhatsApp v. NSO Group*,” *Berkeley Technology Law Journal*, v. 36, n. 1, 2021.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague, C. Troncoso, “Bugs in our Pockets: The Risks of Client-Side Scanning,” arXiv:2110.07450 [cs.CR], October 14, 2021.

N. E. Sanders and B. Schneier, “Machine Learning Featurizations for AI Hacking of Political Systems,” arXiv:2110.09231 [cs.CY], October 8, 2021.

H. Farrell and B. Schneier, “Rechanneling Beliefs: How Information Flows Hinder or Help Democracy,” Stavros Niarchos Foundation SNF Agora Institute, Johns Hopkins, May 24, 2021.

B. Schneier, “The Coming AI Hackers,” Belfer Center for Science and International Affairs, Harvard Kennedy School, April 2021.

G. Corn, J. Daskal, J. Goldsmith, C. Inglis, P. Rozenzweig, S. Sacks, B. Schneier, A. Stamos, V. Stewart, “Chinese Technology Platforms Operating in the United States: Assessing the Threat,” *Joint Report of the National Security, Technology, and Law*

Bruce Schneier CV: Academic Publications

4

Working Group at the Hoover Institution at Stanford University and the Tech, Law & Security Program at American University Washington College of Law, February 11, 2021.

R. S. S. Kumar, J. Penney, B. Schneier, K. Albert, “Legal Risks of Adversarial Machine Learning Research,” *arXiv:2006.16179*.

N. Kim, T. Herr, and B. Schneier, “The Reverse Cascade: Enforcing Security on the Global IoT Supply Chain,” *Atlantic Council*, June 2020.

K. Levy and B. Schneier, “Privacy Threats in Intimate Relationships,” *Journal of Cybersecurity*, v. 6, n. 1, 2020.

M. Bourdeaux, G. Abiola, B. Edgar, J. Pershing J. Wang, M. Van Loon, B. Schneier, “Weaponizing Digital Health Intelligence,” *Belfer Center for Science and International Affairs, Harvard Kennedy School*, January 2020.

K. Albert, J. Penney, B. Schneier, R. Shankar, and S. Kumar, “Politics of Adversarial Machine Learning,” *arXiv:2002.05648*, February 2020.

A. Adams, F. Ben-Youssef, B. Schneier, K. Murata, “Superheroes on Screen: Real Life Lessons for Security Debates,” *Security Journal*, 2019.

H. Farrell, B. Schneier, “Common-Knowledge Attacks on Democracy,” Berkman Klein Center Research Publication No. 2018-7, October 2018.

T. Herr, B. Schneier, and C. Morris, “Taking Stock: Estimating Vulnerability Rediscovery,” July 2017 (revised October 2017).

O. S. Kerr, B. Schneier, “Encryption Workarounds,” March 2017.

S. Shackelford, B. Schneier, M. Sulmeyer, A. Boustead, B. Buchanan, A. Craig, T. Herr, and J. Z. Malekos Smith, “Making Democracy Harder to Hack: Should Elections Be Classified as ‘Critical Infrastructure’?,” *University of Michigan Journal of Law Reform*, v. 50, n. 3, Spring 2017, pp. 629–668.

J. Quinn and B. Schneier, “A Proportional Voting System for Awards Nominations Resistant to Voting Blocs,” *Voting Matters*, n. 31, to appear.

B. Schneier, K. Seidel, S. Vijayakumar, “A Worldwide Survey of Encryption Products,” Berkman Center Report, February 11, 2016.

U. Gasser, M. G. Olsen, N. Gertner, D. Renan, J. Goldsmith, J. Sanchez, S. Landau, B. Schneier, J. Nye, L. Schwartzol, D. R. O’Brien, J. Zittrain, “Don’t Panic: Making Progress on the ‘Going Dark’ Debate,” Berkman Center Report, February 1, 2016.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, D.

- J. Weitzner, “Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications,” *Journal of Cybersecurity*, November 2015.
- B. Schneier, M. Fredrikson, T. Kohno, T. Ristenpart, “Surreptitiously Weakening Cryptographic Systems,” *Cryptology ePrint Archive Report 2015/097*, 2015.
- A. Czeskis, D. Mah, O. Sandoval, I. Smith, K. Koscher, J. Appelbaum, T. Kohno, B. Schneier, “DeadDrop/Strongbox Security Assessment,” *UW Computer Science and Engineering Technical Report #13-08-02*, August 8, 2013.
- B. Schneier, “Schneier on Security: Privacy and Control,” *Journal of Privacy and Confidentiality*, v.2, n.1, pp. 3–4, 2010.
- N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, J. Walker, “The Skein Hash Function Family,” version 1.2, September 15, 2009.
- M. Bellare, T. Kohno, S. Lucks, N. Ferguson, B. Schneier, D. Whiting, J. Callas, J. Walker, “Provable Security Support for the Skein Hash Family,” April 29, 2009.
- A. Czeskis, D. J. St. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, and B. Schneier, “Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications,” 3rd Usenix Workshop on Hot Topics in Security, 2008.
- B. Schneier, “The Psychology of Security,” *AFRICACRYPT 2008, LNCS 5023*, Springer-Verlag, 2008, pp. 50–79.
- R. Anderson and B. Schneier, “Economics of Information Security,” *IEEE Security and Privacy* 3 (1), 2005, pp. 12–13.
- J. Kelsey and B. Schneier, “Second Preimages on n -bit Hash Functions for Much Less than 2^n Work,” *Advances in Cryptology: EUROCRYPT 2005 Proceedings*, Springer-Verlag, 2005, pp. 474–490.
- D. Whiting, B. Schneier, S. Lucks, and F. Muller, “Phelix: Fast Encryption and Authentication in a Single Cryptographic Primitive,” *ECRYPT Stream Cipher Project Report 2005/027*.
- N. Ferguson and B. Schneier, “A Cryptographic Evaluation of IPsec,” December 2003.
- N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks, and T. Kohno, “Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive,” *Proceedings of Fast Software Encryption 2003*, pp. 345–362.
- K. Jallad, J. Katz, and B. Schneier, “Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG,” *Information Security Conference 2002 Proceedings*, Springer-Verlag, 2002.
- B. Schneier, “Inside Risks 129: Cyber Underwriters Lab?,” *Communications of the ACM*, vol 44, n 4, Apr 2001.

Bruce Schneier CV: Academic Publications**6**

N. Ferguson, J. Kelsey, B. Schneier, M. Stay, D. Wagner, and D. Whiting, “Improved Cryptanalysis of Rijndael,” *Seventh Fast Software Encryption Workshop*, Springer-Verlag, 2001, pp. 213–230.

J. Kelsey, T. Kohno, and B. Schneier, “Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent,” *Seventh Fast Software Encryption Workshop*, Springer-Verlag, 2001, pp. 7–93.

J. Kelsey and B. Schneier, “The Street Performer Protocol and Digital Copyrights,” *First Monday*, v. 45, n. 6 (June 2001).

J. Katz and B. Schneier, “A Chosen Ciphertext Attack against Several E-Mail Encryption Protocols,” 9th USENIX Security Symposium, 2000.

B. Schneier, “The Fallacy of Trusted Client Software” (Cryptorhythms column), *Information Security Magazine*, August 2000.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, “The Twofish Team’s Final Comments on AES Selection,” May 15, 2000.

D. Whiting, B. Schneier, S. Bellovin, “AES Key Agility Issues in High-Speed IPsec Implementations,” May 15, 2000.

B. Schneier, “The Process of Security,” *Information Security Magazine*, April 2000.

N. Ferguson, B. Schneier, and D. Wagner, “Security Weaknesses in Maurer-Like Randomized Stream Ciphers,” *Fifth Australasian Conference on Information Security and Privacy* (ACISP 2000), Springer-Verlag, 2000, pp. 234–241.

J. Kelsey and B. Schneier, “MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants,” *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 169–185.

T. Kohno, J. Kelsey, and B. Schneier, “Preliminary Cryptanalysis of Reduced-Round Serpent,” *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 195–211.

B. Schneier and D. Whiting, “A Performance Comparison of the Five AES Finalists,” *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 123–135.

N. Ferguson, J. Kelsey, B. Schneier, D. Whiting, “A Twofish Retreat: Related-Key Attacks Against Reduced-Round Twofish,” Twofish Technical Report #6, February 14, 2000.

C. Ellison and B. Schneier, “Inside Risks 116: Risks of PKI: Electronic Commerce,” *Communications of the ACM*, vol 43, n 2, Feb 2000.

C. Ellison and B. Schneier, “Inside Risks 115: Risks of PKI: Secure E-Mail,” *Communications of the ACM*, vol 43, n 1, Jan 2000.

Bruce Schneier CV: Academic Publications

7

C. Ellison and B. Schneier, “Ten Risks of PKI: What You’re Not Being Told about Public Key Infrastructure,” *Computer Security Journal*, v 16, n 1, 2000, pp. 1–7.

C. Ellison, C. Hall, R. Milbert, and B. Schneier, “Protecting Secret Keys with Personal Entropy,” *Future Generation Computer Systems*, v. 16, 2000, pp. 311–318.

B. Schneier, “Self-Study Course in Block Cipher Cryptanalysis,” *Cryptologia*, v.24, n.1, Jan 2000, pp. 18–34.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Side Channel Cryptanalysis of Product Ciphers,” *Journal of Computer Security*, v. 8, n. 2–3, 2000, pp. 141–158.

J. Kelsey and B. Schneier, “Key-Schedule Cryptanalysis of DEAL,” *Sixth Annual Workshop on Selected Areas in Cryptography* (SAC 99), Springer Verlag, 2000, pp. 118–134.

J. Kelsey, B. Schneier, and N. Ferguson, “Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator,” *Sixth Annual Workshop on Selected Areas in Cryptography* (SAC 99), Springer Verlag, 2000, pp. 13–33.

B. Schneier, “Attack Trees,” *Dr. Dobbs’s Journal*, v. 24, n. 12, Dec 1999, pp. 21–29.

B. Schneier, “The 1999 Crypto Year-in-Review,” *Information Security Magazine*, January 1999.

B. Schneier, “Security in the Real World: How to Evaluate Security Technology,” *Computer Security Journal*, v 15, n 4, 1999, pp. 1–14.

B. Schneier, “A Plea for Simplicity,” *Information Security Magazine*, November 1999.

B. Schneier and Mudge, “Cryptanalysis of Microsoft’s PPTP Authentication Extensions (MS-CHAPv2),” *CQRE ’99*, Springer-Verlag, 1999, pp. 192–203.

B. Schneier, “Inside Risks 112: Risks of Relying on Cryptography,” *Communications of the ACM*, vol 42, n 10, Oct 1999.

B. Schneier, “Inside Risks 111: The Trojan Horse Race,” *Communications of the ACM*, vol 42, n 9, September 1999.

B. Schneier, “International Cryptography,” *Information Security Magazine*, September 1999.

J. Kelsey and B. Schneier, “Minimizing Bandwidth for Remote Access to Cryptographically Protected Audit Logs,” *Second International Workshop on the Recent Advances in Intrusion Detection* (RAID ’99), September 1999.

B. Schneier, “Inside Risks 110: Biometrics: Uses and Abuses,” *Communications of the ACM*, vol 42, n 8, August 1999.

C. Hall, I. Goldberg, and B. Schneier, "Reaction Attacks Against Several Public-Key Cryptosystems," *Proceedings of Information and Communication Security, ICICS'99*, Springer-Verlag, 1999, pp. 2–12.

B. Schneier and A. Shostack, "Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards," *USENIX Workshop on Smart Card Technology*, USENIX Press, 1999, pp. 175–185.

J. Kelsey and B. Schneier, "Authenticating Secure Tokens Using Slow Memory Access," *USENIX Workshop on Smart Card Technology*, USENIX Press, 1999, pp. 101–106.

D. Whiting, J. Kelsey, B. Schneier, D. Wagner, N. Ferguson, and C. Hall, "Further Observations on the Key Schedule of Twofish," Twofish Technical Report #4, March 16, 1999.

E. Biham, A. Biryukov, N. Ferguson, L. Knudsen, B. Schneier, and A. Shamir, "Cryptanalysis of Magenta," Second AES Candidate Conference, April 1999.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "New Results on the Twofish Encryption Algorithm," Second AES Candidate Conference, April 1999.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Performance Comparison of the AES Submissions," Second AES Candidate Conference, April 1999.

D. Whiting, N. Ferguson, and B. Schneier, "Cryptanalysis of FROG," Second AES Candidate Conference, April 1999.

J. Kelsey, B. Schneier, and D. Wagner, "Key Schedule Weakness in SAFER+," Second AES Candidate Conference, April 1999.

J. Kelsey, B. Schneier, and D. Wagner, "Mod n Cryptanalysis, with Applications Against RC5P and M6, Fast Software Encryption," *Sixth International Workshop Proceedings* (March 1999), Springer-Verlag, 1999, pp. 139–155.

B. Schneier and J. Kelsey, "Secure Audit Logs to Support Computer Forensics," *ACM Transactions on Information and System Security*, v. 2, n. 2, May 1999, pp. 159–176.

B. Schneier, "The 1998 Crypto Year-in-Review," *Information Security Magazine*, January 1999.

J. Riordan and B. Schneier, "A Certified E-Mail Protocol with No Trusted Third Party," *13th Annual Computer Security Applications Conference*, ACM Press, December 1998, pp. 347–351.

B. Schneier, "Cryptographic Design Vulnerabilities," *IEEE Computer*, v. 31, n. 9, Sep 1998, pp. 29–33.

B. Schneier and Mudge, “Cryptanalysis of Microsoft’s Point-to-Point Tunneling Protocol (PPTP),” *Proceedings of the 5th ACM Conference on Communications and Computer Security*, ACM Press, November 1998, pp. 132–141.

J. Kelsey and B. Schneier, “The Street Performer Protocol,” *The Third USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1998.

B. Schneier, “Scrambled Message,” *Information Security Magazine*, October 1998.

C. Salter, O.S. Saydjari, B. Schneier, and J. Wallner, “Towards a Secure System Engineering Methodology,” *New Security Paradigms Workshop*, September 1998, pp. 2–10.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Side Channel Cryptanalysis of Product Ciphers,” *ESORICS ’98 Proceedings*, Springer-Verlag, September 1998, pp. 97–110.

C. Hall, J. Kelsey, V. Rijmen, B. Schneier, and D. Wagner, “Cryptanalysis of SPEED,” *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 319–338.

D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, “Cryptanalysis of ORYX,” *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 296–305.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, and C. Hall, “On the Twofish Key Schedule,” *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 27–42.

C. Hall, J. Kelsey, B. Schneier, and D. Wagner, “Building Pseudo-Random Functions from Pseudo-Random Permutations,” *Advances in Cryptology—CRYPTO ’98 Proceedings*, Springer-Verlag, August 98, pp. 370–389.

J. Riordan and B. Schneier, “Environmental Key Generation towards Clueless Agents,” *Mobile Agents and Security*, G. Vigna, ed., Springer-Verlag, 1998, pp. 15–24.

C. Hall, J. Kelsey, B. Schneier, and D. Wagner, “Cryptanalysis of SPEED (Extended Abstract),” *Financial Cryptography ’98*, Springer-Verlag, 1998, 309–310.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, “Twofish: A 128-Bit Block Cipher,” 15 June 1998.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Cryptanalytic Attacks on Pseudorandom Number Generators,” *Fast Software Encryption, Fifth International Workshop Proceedings* (March 1998), Springer-Verlag, 1998, pp. 168–188.

D. Coppersmith, D. Wagner, B. Schneier, and J. Kelsey, “Cryptanalysis of TwoPrime,” *Fast Software Encryption, Fifth International Workshop Proceedings* (March 1988), Springer-Verlag, 1998, 32–48.

B. Schneier and J. Kelsey, "Cryptographic Support for Secure Logs on Untrusted Machines," *The Seventh USENIX Security Symposium Proceedings*, USENIX Press, January 1998, pp. 53–62.

J. Kelsey, B. Schneier, C. Hall, and D. Wagner, "Secure Applications of Low-Entropy Keys," *1997 Information Security Workshop (ISW'97)*, Proceedings (September 1997), Springer-Verlag, 1998, pp. 121–134.

B. Schneier and C. Hall, "An Improved E-mail Security Protocol," *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 232–238.

C. Hall and B. Schneier, "Remote Electronic Gambling," *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 227–230.

J. Kelsey, B. Schneier, and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA," *ICICS '97 Proceedings*, Springer-Verlag, November 1997, pp. 233–246.

D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm," *Advances in Cryptology—CRYPTO '97 Proceedings*, Springer-Verlag, August 1997, pp. 526–537.

N. Ferguson and B. Schneier, "Cryptanalysis of Akelarre," *Fourth Annual Workshop on Selected Areas in Cryptography*, August 1997, pp. 201–212.

H. Abelson, R. Anderson, S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R.L. Rivest, J.I. Schiller, and B. Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," *World Wide Web Journal*, v.2, n.3, 1997, pp. 241–257.

J. Kelsey and B. Schneier, "Conditional Purchase Orders," *4th ACM Conference on Computer and Communications Security*, ACM Press, April 1997, pp. 117–124.

J. Kelsey, B. Schneier, and D. Wagner, "Protocol Interactions and the Chosen Protocol Attack," *Security Protocols, International Workshop April 1997 Proceedings*, Springer-Verlag, 1998, pp. 91–104.

B. Schneier and J. Kelsey, "Remote Auditing of Software Outputs Using a Trusted Coprocessor," *Journal of Future Generation Computer Systems*, v.13, n.1, 1997, pp. 9–18.

B. Schneier, "Why Cryptography is Harder than it Looks," *Information Security Bulletin*, v. 2, n. 2, March 1997, pp. 31–36.

B. Schneier and D. Whiting, "Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor," *Fast Software Encryption, Fourth International Workshop Proceedings* (January 1997), Springer-Verlag, 1997, pp. 242–259.

B. Schneier, "Cryptography, Security, and the Future," *Communications of the ACM*, v. 40, n. 1, January 1997, p. 138.

J. Kelsey, B. Schneier, and C. Hall, "An Authenticated Camera," *12th Annual Computer Security Applications Conference*, ACM Press, December 1996, pp. 24–30.

B. Schneier and J. Kelsey, "A Peer-to-Peer Software Metering System," *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 279–286.

D. Wagner and B. Schneier, "Analysis of the SSL 3.0 Protocol," *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 29–40.

B. Schneier, J. Kelsey, and J. Walker, "Distributed Proctoring," *ESORICS 96 Proceedings*, Springer-Verlag, September 1996, pp. 172–182.

J. Kelsey and B. Schneier, "Authenticating Outputs of Computer Software Using a Cryptographic Coprocessor," *Proceedings 1996 CARDIS*, September 1996, pp. 11–24.

J. Kelsey, B. Schneier, and D. Wagner, "Key-Schedule Cryptanalysis of 3-WAY, IDEA, G-DES, RC4, SAFER, and Triple-DES," *Advances in Cryptology—CRYPTO '96 Proceedings*, Springer-Verlag, August 1996, pp. 237–251.

B. Schneier and J. Kelsey, "Automatic Event Stream Notarization Using Digital Signatures," *Security Protocols, International Workshop April 1996 Proceedings*, Springer-Verlag, 1997, pp. 155–169.

B. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block Cipher Design," *Fast Software Encryption, Third International Workshop Proceedings* (February 1996), Springer-Verlag, 1996, pp. 121–144.

M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," January 1996.

M. Jones and B. Schneier, "Securing the World Wide Web: Smart Tokens and their Implementation," *Proceedings of the Fourth International World Wide Web Conference*, December 1995, pp. 397–409.

B. Schneier, "Blowfish—One Year Later," *Dr. Dobb's Journal*, September 1995.

M. Blaze and B. Schneier, "The MacGuffin Block Cipher Algorithm," *Fast Software Encryption, Second International Workshop Proceedings* (December 1994), Springer-Verlag, 1995, pp. 97–110.

B. Schneier, "The GOST Encryption Algorithm," *Dr. Dobb's Journal*, v. 20, n. 1, January 1995, pp. 123–124.

Bruce Schneier CV: Selected Awards**12**

B. Schneier, “A Primer on Authentication and Digital Signatures,” *Computer Security Journal*, v. 10, n. 2, 1994, pp. 38–40.

B. Schneier, “Designing Encryption Algorithms for Real People,” *Proceedings of the 1994 ACM SIGSAC New Security Paradigms Workshop*, IEEE Computer Society Press, August 1994, pp. 63–71.

B. Schneier, “The Blowfish Encryption Algorithm,” *Dr. Dobbs’s Journal*, v. 19, n. 4, April 1994, pp. 38–40.

B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish),” *Fast Software Encryption, Cambridge Security Workshop Proceedings* (December 1993), Springer-Verlag, 1994, pp. 191–204.

B. Schneier, “One-Way Hash Functions,” *Dr. Dobbs’s Journal*, v. 16, n. 9, September 1991, pp. 148–151.

Selected Awards

Schneier on Security listed as one of the Cyber Security Blogs You Need to See, Focus Training, February 2017.

Business Leader in Cybersecurity Award from Boston Global Forum, December 2015.

Named as one of the 20 top security influencers by *eSecurity Planet*, June 2015.

EPIC Lifetime Achievement Award, June 2015.

Named as one of the top ten information security bloggers of 2014 by the ISO 27001 and ISO 22301 blog, December 2014.

Named as an industry pioneer in information security by *SC Magazine*, December 2014.

Berkman Fellow at the Berkman Center for Internet and Society at Harvard University, 2013–2015 academic years.

Named one of the IFSEC 40: The Most Influential People in Security & Fire, January 2013.

Honorary Doctor of Science (ScD) from University of Westminster, London, December 2011.

CSO Compass Award, May 2010.

Named as one of the top 25 most influential people in the security industry by *Security* magazine, December 2008

Inducted into the Infosecurity Europe Hall of Fame, April 2008.

Bruce Schneier CV: Legislative Testimony

13

Computer Professionals for Social Responsibility (CPSR) Norbert Wiener Award, January 2008.

Electronic Frontier Foundation (EFF) Pioneer Award, March 2007.

Dr. Dobb's Journal Excellence in Programming Award, April 2006.

Named as one of the top five influential IT security thinkers by SC magazine, December 2005.

Infoworld CTO 25 Award, April 2005.

Secrets and Lies won a Productivity Award in the 13th Annual *Software Development Magazine* Product Excellence Awards, 2000.

Legislative Testimony

Letter to the US Senate Judiciary Committee in support of S.2992 and S.2710, January 31, 2022.

Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection, hearing on “Securing Consumers’ Credit Data in the Age of Digital Commerce,” November 1, 2017.

Testimony at the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Communications and Technology, and the Subcommittee on Commerce, Manufacturing, and Trade, hearing on “Understanding the Role of Connected Devices in Recent Cyber Attacks,” November 16, 2016.

Testimony before the U.S. Senate Judiciary Committee, hearing on “Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns,” May 8, 2007.

Testimony at the U.K. House of Lords Science and Technology Committee inquiry into “Personal Internet Security,” February 21, 2007.

Testimony before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research and Development, hearing on “Overview of the Cyber Problem—A Nation Dependent and Dealing with Risk,” June 25, 2003.

Testimony before the U.S. Senate Committee on Commerce, Science and Transportation, Subcommittee on Science, Technology, and Space, hearing on Internet Security, July 16, 2001.

Published Articles

“How to Decarbonize Crypto,” *Atlantic*, December 6, 2022.

“Centralized vs. Decentralized Data Systems—Which Choice Is Best?” *VentureBeat*, September 12, 2022.

“NIST’s Post-Quantum Cryptography Standards Competition,” *IEEE Security & Privacy*, August 7, 2022.

“When Corporate Interests and International Cyber Agreements Collide,” *Cipher Brief*, May 5, 2022.

“Why Vaccine Cards Are So Easily Forged,” *The Atlantic*, March 8, 2022.

“Letter to the US Senate Judiciary Committee on App Stores,” January 31, 2022.

“Robot Hacking Games,” *IEEE Security & Privacy*, January 1, 2022.

“How to Cut Down on Ransomware Attacks Without Banning Bitcoin,” *Slate*, June 17, 2021.

“Hacked Drones and Busted Logistics Are the Cyber Future of Warfare,” *Brookings TechStream*, June 5, 2021.

“Russia’s Hacking Success Shows How Vulnerable the Cloud Is,” *Foreign Policy*, May 24, 2021.

“‘Grassroots’ Bot Campaigns Are Coming. Governments Don’t Have a Plan to Stop Them.,” *The Washington Post*, May 20, 2021.

“Hackers Used to Be Humans. Soon, AIs Will Hack Humanity,” *Wired*, April 19, 2021.

“Bitcoin’s Greatest Feature Is Also Its Existential Threat,” *Wired*, March 9, 2021.

“Illuminating SolarStorm: Implications for National Strategy and Policy,” *Aspen Institute*, March 04, 2021.

“Why Was SolarWinds So Vulnerable to a Hack?” *New York Times*, February 23, 2021.

“The Government Will Guard Biden’s Peloton from Hackers. What About the Rest of Us?,” *The Washington Post*, February 2, 2021.

“The Solarwinds Hack Is Stunning. Here’s What Should Be Done,” *CNN*, January 5, 2021.

Bruce Schneier CV: Published Articles**15**

“Audio: Firewalls Don’t Stop Dragons Podcast,” *Firewalls Don't Stop Dragons*, December 28, 2020.

“Audio: The Hack by Russia Is Huge. Here’s Why It Matters.,” *MPR News*, December 28, 2020.

“Review of Data and Goliath (German),” *Nerdhalla*, December 27, 2020.

“Video: The Most Consequential Cyber-Attack in History Just Happened. What Now?,” *LA Times*, December 24, 2020.

“Video: AshbrookLIVE #14 – Bruce Schneier,” *AshbrookLIVE*, December 24, 2020.

“Audio: Full Disclosure with Bruce Schneier,” *BarCode*, December 20, 2020.

“Audio: How Your Digital Footprint Makes You the Product,” *TechSequences*, December 16, 2020.

“Video: Hack in the Box Security Conference Keynote Interview,” *Hack In The Box Security Conference*, December 3, 2020.

“Video: Election Security: Securing the Vote While Securing the System,” *The Legal Edition*, November 19, 2020.

“#ISC2Congress: Modern Security Pros Are Much More than Technologists, Says Bruce Schneier,” *Infosecurity*, November 18, 2020.

“Audio: Ballot Question 1: Risks & Regulations Regarding Right to Repair,” *Pioneer Institute*, October 13, 2020.

“Audio: We Live in a Security and Privacy World that Science Fiction Didn’t Predict,” *OWASP PDX Podcast*, October 4, 2020.

“How Amazon and Walmart Could Fix IoT Security,” *Data Breach Today*, June 26, 2020.

“The Cyberflâneur #29: Bruce Schneier,” *The Syllabus*, June 16, 2020.

“Audio: Interview with Bruce Schneier for Blockchain Rules Podcast Series,” *Blockchain Rules Podcast*, June 16, 2020.

“Audio: Is Contact Tracing Dumb? False Positives, Loss of Trust, and an Uncertain Path Back to Normalcy,” *Policy Punchline*, June 2, 2020.

“Coronavirus, il guru Bruce Schneier: «Le app di contact tracing? Inutili. Margini di errore troppo alti»,” *Open*, June 2, 2020.

“Audio: Click Here to Kill Everybody: Security and Survival in a Hyper-connected World,” *Policy Punchline*, May 29, 2020.

Bruce Schneier CV: Published Articles**16**

“Audio: Bruce Schneier on Truth, Reality, and Contact Tracing,” *Reality 2.0*, May 27, 2020.

“Video: Public Interest Technologists—Interview with Bruce Schneier and Jon Callas,” *Cyber Cyber Cyber Cyber*, May 19, 2020.

“The Public Good Requires Private Data,” *Foreign Policy*, May 16, 2020.

“How Hackers and Spies Could Sabotage the Coronavirus Fight,” *Foreign Policy*, February 28, 2020.

“Technologists vs. Policy Makers,” *IEEE Security & Privacy*, January/February 2020.

“We’re Banning Facial Recognition. We’re Missing the Point.,” *The New York Times*, January 20, 2020.

“China Isn’t the Only Problem With 5G,” *Foreign Policy*, January 10, 2020.

“Bots Are Destroying Political Discourse As We Know It,” *The Atlantic*, January 7, 2020.

“We Must Bridge the Gap Between Technology and Policymaking. Our Future Depends on It,” *World Economic Forum*, November 12, 2019.

“Every Part of the Supply Chain Can Be Attacked,” *The New York Times*, September 25, 2019.

“The Real Threat from China Isn’t ‘Spy Trains,’” *CNN*, September 21, 2019.

“What Digital Nerds and Bio Geeks Have to Worry About,” *CNN*, September 13, 2019.

“The Myth of Consumer Security,” *Lawfare*, August 26, 2019.

“8 Ways to Stay Ahead of Influence Operations,” *Foreign Policy*, August 12, 2019.

“Attorney General William Barr on Encryption Policy,” *Lawfare*, July 23, 2019.

“We Must Prepare for the Next Pandemic,” *The New York Times*, June 17, 2019.

“AI Has Made Video Surveillance Automated and Terrifying,” *Motherboard*, June 13, 2019.

“AI Can Thrive in Open Societies,” *Foreign Policy*, June 13, 2019.

“When Fake News Comes to Academia,” *Lawfare*, May 24, 2019.

“Democracy’s Dilemma,” *Boston Review*, May 15, 2019.

“Russia’s Attacks on Our Democratic Systems Call for Diverse Countermeasures,” *The Hill*, May 7, 2019.

“Toward an Information Operations Kill Chain,” *Lawfare*, April 24, 2019.

Bruce Schneier CV: Published Articles

17

“A New Privacy Constitution for Facebook,” *OneZero*, March 8, 2019.

“Cybersecurity for the Public Interest,” *IEEE Security & Privacy*, January/February 2019.

“There’s No Good Reason to Trust Blockchain Technology,” *Wired*, February 6, 2019.

“The Public-Interest Technologist Track at the RSA Conference,” *RSA Conference Blogs*, January 29, 2019.

“Defending Democratic Mechanisms and Institutions against Information Attacks,” *Defusing Disinfo*, January 28, 2019.

“Evaluating the GCHQ Exceptional Access Proposal,” *Lawfare*, January 17, 2019.

“Machine Learning Will Transform How We Detect Software Vulnerabilities,” *SecurityIntelligence*, December 18, 2018.

“The Most Damaging Election Disinformation Campaign Came From Donald Trump, Not Russia,” *Motherboard*, November 19, 2018.

“Surveillance Kills Freedom By Killing Experimentation,” *Wired*, November 16, 2018.

“Information Attacks on Democracies,” *Lawfare*, November 15, 2018.

“We Need Stronger Cybersecurity Laws for the Internet of Things,” *CNN*, November 9, 2018.

“Nobody’s Cellphone Is Really That Secure,” *The Atlantic*, October 26, 2018.

“Internet Hacking Is About to Get Much Worse,” *New York Times*, October 11, 2018.

“Cryptography after the Aliens Land,” *IEEE Security & Privacy*, September/October 2018.

“Don’t Fear the TSA Cutting Airport Security. Be Glad That They’re Talking about It,” *Washington Post*, August 17, 2018.

“Censorship in the Age of Large Cloud Providers,” *Lawfare*, June 7, 2018.

“Why the FBI Wants You to Reboot Your Router — and Why That Won’t Be Enough Next Time,” *The Washington Post*, June 6, 2018.

“Data Protection Laws Are Shining a Needed Light on a Secretive Industry,” *The Guardian*, June 1, 2018.

“What ‘Efail’ Tells Us About Email Vulnerabilities and Disclosure,” *Lawfare*, May 24, 2018.

“Banning Chinese Phones Won’t Fix Security Problems with Our Electronic Supply Chain,” *The Washington Post*, May 8, 2018.

“American Elections Are Too Easy to Hack. We Must Take Action Now,” *The Guardian*, April 18, 2018.

“It’s Not Just Facebook. Thousands of Companies are Spying on You,” *CNN*, March 26, 2018.

“Artificial Intelligence and the Attack/Defense Balance,” *IEEE Security & Privacy*, March/April 2018.

“Can Consumers’ Online Data Be Protected?,” *CQ Researcher*, February 9, 2018.

“How to Fight Mass Surveillance Even Though Congress Just Reauthorized It,” *The Washington Post*, January 25, 2018.

“The New Way Your Computer Can Be Attacked,” *The Atlantic*, January 22, 2018.

“The Security of Pretty Much Every Computer on the Planet Has Just Gotten a Lot Worse,” *CNN*, January 5, 2018.

“How the Supreme Court Could Keep Police From Using Your Cellphone to Spy on You,” *The Washington Post*, November 27, 2017.

“Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection,” , November 1, 2017.

“Don’t Waste Your Breath Complaining to Equifax about Data Breach ,” *CNN*, September 11, 2017.

“IoT Security: What’s Plan B?,” *IEEE Security & Privacy*, September/October 2017.

“‘Twitter and Tear Gas’ Looks at How Protest Is Fueled and Crushed by the Internet,” *Motherboard*, July 11, 2017.

“Why the NSA Makes Us More Vulnerable to Cyberattacks,” *Foreign Affairs*, May 30, 2017.

“Who Are the Shadow Brokers?,” *The Atlantic*, May 23, 2017.

“What Happens When Your Car Gets Hacked?,” *The New York Times*, May 19, 2017.

“Why Extending Laptop Ban Makes No Sense,” *CNN*, May 16, 2017.

“The Next Ransomware Attack Will Be Worse than WannaCry,” *The Washington Post*, May 16, 2017.

“Three Lines of Defense against Ransomware Attacks,” *New York Daily News*, May 15, 2017.

“Online Voting Won’t Save Democracy,” *The Atlantic*, May 10, 2017.

“Who Is Publishing NSA and CIA Secrets, and Why?,” *Lawfare*, April 27, 2017.

“The Quick vs the Strong: Commentary on Cory Doctorow’s *Walkaway*,” *Crooked Timber*, April 26, 2017.

“Infrastructure Vulnerabilities Make Surveillance Easy,” *Al Jazeera*, April 11, 2017.

“Snoops May Soon Be Able to Buy Your Browsing History. Thank the US Congress,” *The Guardian*, March 30, 2017.

“Puzzling out TSA’s Laptop Travel Ban,” *CNN*, March 22, 2017.

“Security Orchestration for an Uncertain World,” *SecurityIntelligence*, March 21, 2017.

“How to Keep Your Private Conversations Private for Real,” *The Washington Post*, March 8, 2017.

“Botnets of Things,” *MIT Technology Review*, March/April 2017.

“Click Here to Kill Everyone,” *New York Magazine*, January 27, 2017.

“Why Proving the Source of a Cyberattack is So Damn Difficult,” *CNN*, January 5, 2017.

“Class Breaks,” *Edge*, December 30, 2016.

“U.S. Elections Are a Mess, Even Though There’s No Evidence This One Was Hacked,” *The Washington Post*, November 23, 2016.

“Testimony at the U.S. House of Representatives Joint Hearing ‘Understanding the Role of Connected Devices in Recent Cyber Attacks,’” November 16, 2016.

“American Elections Will Be Hacked,” *The New York Times*, November 9, 2016.

“Your WiFi-Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations,” *The Washington Post*, November 3, 2016.

“Lessons From the Dyn DDoS Attack,” *SecurityIntelligence*, November 1, 2016.

“Cybersecurity Issues for the Next Administration,” *Time*, October 13, 2016.

“We Need to Save the Internet from the Internet of Things,” *Motherboard*, October 6, 2016.

“How Long Until Hackers Start Faking Leaked Documents?,” *The Atlantic*, September 13, 2016.

“Someone Is Learning How to Take Down the Internet,” *Lawfare*, September 13, 2016.

“Stop Trying to Fix the User,” *IEEE Security & Privacy*, September/October 2016.

Bruce Schneier CV: Published Articles**20**

“New Leaks Prove It: The NSA Is Putting Us All at Risk to Be Hacked,” *Vox*, August 24, 2016.

“Hackers Are Putting U.S. Election at Risk,” *CNN*, July 28, 2016.

“By November, Russian Hackers Could Target Voting Machines,” *The Washington Post*, July 27, 2016.

“The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters,” *Motherboard*, July 25, 2016.

“Credential Stealing as Attack Vector,” *Xconomy*, April 20, 2016.

“The Value of Encryption,” *The Ripon Forum*, April 2016.

“Can You Trust IRS to Keep Your Tax Data Secure?,” *CNN*, April 13, 2016.

“Your iPhone Just Got Less Secure. Blame the FBI.,” *The Washington Post*, March 29, 2016.

“Cryptography Is Harder Than It Looks,” *IEEE Security & Privacy*, January/February 2016.

“Data Is a Toxic Asset, So Why Not Throw It Out?,” *CNN*, March 1, 2016.

“A ‘Key’ for Encryption, Even for Good Reasons, Weakens Security,” *The New York Times Room for Debate*, February 23, 2016.

“Why You Should Side With Apple, Not the FBI, in the San Bernardino iPhone Case,” *The Washington Post*, February 18, 2016.

“Candidates Won’t Hesitate to Use Manipulative Advertising to Score Votes,” *The Guardian*, February 4, 2016.

“The Internet Of Things Will Be The World’s Biggest Robot,” *Forbes*, February 2, 2016.

“Security vs. Surveillance,” *Don’t Panic: Making Progress on the ‘Going Dark’ Debate*, February 1, 2016.

“When Hacking Could Enable Murder,” *CNN*, January 26, 2016.

“How an Overreaction to Terrorism Can Hurt Cybersecurity,” *MIT Technology Review*, January 25, 2016.

“The Internet of Things That Talk About You Behind Your Back,” *Motherboard*, January 8, 2016.

“The Risks—and Benefits—of Letting Algorithms Judge Us,” *CNN*, January 6, 2016.

Bruce Schneier CV: Published Articles**21**

“How the Internet of Things Limits Consumer Choice,” *The Atlantic*, December 24, 2015.

“Can Laws Keep Up with Tech World?,” *CNN*, December 21, 2015.

“The Automation of Reputation,” *Edge.org*, November 5, 2015.

“The Rise of Political Doxing,” *Motherboard*, October 28, 2015.

“Face Facts about Internet Security,” *CNN*, October 23, 2015.

“The Era Of Automatic Facial Recognition And Surveillance Is Here, *Forbes*, September 29, 2015.

“Stealing Fingerprints,” *Motherboard*, September 29, 2015.

“VW Scandal Could Just Be the Beginning,” *CNN*, September 28, 2015.

“Living in Code Yellow,” *Fusion*, September 22, 2015.

“Hacking Team, Computer Vulnerabilities, and the NSA,” *Georgetown Journal of International Affairs*, September 13, 2015.

“Is It OK to Shoot Down a Drone over Your Backyard?” *CNN*, September 9, 2015.

“The Meanest Email You Ever Wrote, Searchable on the Internet,” *Atlantic*, September 8, 2015.

“Should Some Secrets Be Exposed?” *CNN*, July 7, 2015.

“Why We Encrypt,” Foreword to Privacy International’s *Securing Safe Spaces Online*, June 2015.

“China and Russia Almost Definitely Have the Snowden Docs,” *Wired*, June 16, 2015

“Why are We Spending \$7 Billion on TSA?” *CNN*, June 5, 2015

“Debate: Should Companies Do Most of Their Computing in the Cloud?” *The Economist*, June 5, 2015

“How We Sold Our Souls—and More—to the Internet Giants,” *The Guardian*, May 17, 2015

“Could Your Plane Be Hacked?” *CNN*, April 16, 2015

“Baseball’s New Metal Detectors Won’t Keep You Safe. They’ll Just Make You Miss a Few Innings,” *The Washington Post*, April 14, 2015

“The Big Idea: *Data and Goliath*,” *Whatever*, March 4, 2015.

Bruce Schneier CV: Published Articles**22**

“Hacker or Spy? In Today’s Cyberattacks, Finding the Culprit Is a Troubling Puzzle,” *The Christian Science Monitor*, March 4, 2015.

“The World’s Most Sophisticated Hacks: Governments?,” *Fortune*, March 3, 2015.

“Cyberweapons Have No Allegiance,” *Motherboard*, February 25, 2015.

“Everyone Wants You To Have Security, But Not from Them,” *Forbes*, February 23, 2015.

“Your TV May Be Watching You,” *CNN*, February 11, 2015.

“When Thinking Machines Break The Law,” *Edge*, January 28, 2015.

“The Importance of Deleting Old Stuff—Another Lesson From the Sony Attack,” *Ars Technica*, January 12, 2015.

“The Government Must Show Us the Evidence That North Korea Attacked Sony,” *Time*, January 5, 2015.

“We Still Don’t Know Who Hacked Sony,” *The Atlantic*, January 5, 2015.

“2015: The Year ‘Doxing’ Will Hit Home,” *BetaBoston*, December 31, 2014.

“Did North Korea Really Attack Sony?,” *The Atlantic*, December 22, 2014.

“Sony Made It Easy, but Any of Us Could Get Hacked,” *The Wall Street Journal*, December 19, 2014.

“The Best Thing We Can Do About the Sony Hack Is Calm Down,” *Motherboard*, December 19, 2014.

“What Are the Limits of Police Subterfuge?,” *The Atlantic*, December 17, 2014.

“Over 700 Million People Taking Steps to Avoid NSA Surveillance,” *Lawfare*, December 15, 2014.

“NSA Hacking of Cell Phone Networks,” *Lawfare*, December 8, 2014.

“Antivirus Companies Should Be More Open About Their Government Malware Discoveries,” *MIT Technology Review*, December 5, 2014.

“Why Uber’s ‘God View’ Is Creepy,” *CNN*, December 4, 2014.

“Stop the Hysteria over Apple Encryption,” *CNN*, October 3, 2014.

“The Future of Incident Response,” *IEEE Security & Privacy*, September/October 2014.

“The U.S.’s Hypocritical Stance Against Chinese Hackers,” *Time*, May 20, 2014.

“A Human Problem,” *The Mark News*, May 19, 2014.

“Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?,” *The Atlantic*, May 19, 2014.

“Let the Spies Spy, Let the Cops Chase Terrorists,” *CNN*, May 15, 2014.

“Internet Subversion,” *Boston Review*, May/June 2014.

“How Secure are Snapchat-style Apps?,” *CNN*, March 26, 2014.

“Don’t Listen to Google and Facebook: The Public-Private Surveillance Partnership Is Still Going Strong,” *The Atlantic*, March 25, 2014.

“There’s No Real Difference Between Online Espionage and Online Attack,” *The Atlantic*, March 6, 2014.

“Metadata = Surveillance,” *IEEE Security & Privacy*, March/April 2014.

“NSA Robots are ‘Collecting’ Your Data, Too, and They’re Getting Away With It,” *The Guardian*, February 27, 2014.

“Choosing a Secure Password,” *Boing Boing*, February 25, 2014.

“It’s Time to Break Up the NSA,” *CNN*, February 20, 2014.

“Let the NSA Keep Hold of the Data,” *Slate*, February 14, 2014.

“Everything We Know About How the NSA Tracks People’s Physical Location,” *The Atlantic*, February 11, 2014.

“How the NSA Threatens National Security,” *The Atlantic*, January 6, 2014.

“The Internet of Things Is Wildly Insecure—And Often Unpatchable,” *Wired*, January 6, 2014.

“‘Stalker Economy’ Here to Stay,” *CNN*, November 20, 2013.

“A Fraying of the Public/Private Surveillance Partnership,” *The Atlantic*, November 8, 2013.

“Leakers and Governments Should Work Together,” *CNN*, November 4, 2013.

“The Battle for Power on the Internet,” *The Atlantic*, October 24, 2013.

“Why the NSA’s Defense of Mass Data Collection Makes No Sense,” *The Atlantic*, October 21, 2013.

“Your Life, Under Constant Surveillance,” *CNN*, October 16, 2013.

“How to Design—And Defend Against—The Perfect Security Backdoor,” *Wired*, October 16, 2013.

“Want to Evade NSA Spying? Don’t Connect to the Internet,” *Wired*, October 7, 2013.

“How the NSA Thinks About Secrecy and Risk,” *The Atlantic*, October 4, 2013.

“Why the NSA’s Attacks on the Internet Must Be Made Public,” *The Guardian*, October 4, 2013.

“Attacking Tor: How the NSA Targets Users’ Online Anonymity,” *The Guardian*, October 4, 2013.

“NSA and GCHQ target Tor Network That Protects Anonymity of Web Users,” *The Guardian*, October 4, 2013.

“Book Review: Cyber War Will Not Take Place,” *Europe’s World*, October 1, 2013.

“Understanding the Threats in Cyberspace,” *Europe’s World*, September 27, 2013.

“Could U.S. Have Stopped Syria’s Chemical Attack?,” *CNN*, September 11, 2013.

“The NSA-Reform Paradox: Stop Domestic Spying, Get More Security,” *The Atlantic*, September 11, 2013.

“If the New iPhone Has Fingerprint Authentication, Can It Be Hacked?,” *Wired*, September 9, 2013.

“NSA Surveillance: a Guide to Staying Secure,” *The Guardian*, September 6, 2013.

“The Spooks Need New Ways to Keep Their Secrets Safe,” *Financial Times*, September 5, 2013.

“The US Government Has Betrayed the Internet. We Need to Take It Back,” *The Guardian*, September 5, 2013.

“The Only Way to Restore Trust in the NSA,” *The Atlantic*, September 4, 2013.

“How Advanced Is the NSA’s Cryptanalysis—And Can We Resist It?,” *Wired*, September 4, 2013.

“Trust in Man/Machine Security Systems,” *IEEE Security & Privacy*, September/October 2013.

“Syrian Electronic Army: A Brief Look at What Businesses Need to Know,” *The Wall Street Journal*, August 29, 2013.

“NSA Intimidation Expanding Surveillance State,” *USA Today*, August 27, 2013.

“Our Decreasing Tolerance To Risk,” *Forbes*, August 23, 2013.

“The Real, Terrifying Reason Why British Authorities Detained David Miranda,” *The Atlantic*, August 22, 2013.

“How Companies Can Protect Against Leakers,” *Bloomberg.com*, August 21, 2013.

“Why It’s So Easy to Hack Your Home,” *CNN*, August 15, 2013.

“The NSA Is Commandeering the Internet,” *The Atlantic*, August 12, 2013.

“The Army in Our Midst,” *The Wall Street Journal*, August 5, 2013.

“The Public-Private Surveillance Partnership,” *Bloomberg.com*, July 31, 2013.

“NSA Secrets Kill Our Trust,” *CNN*, July 31, 2013.

“Cyberconflicts and National Security,” *UN Chronicle*, July 18, 2013.

“Mission Creep: When Everything Is Terrorism,” *The Atlantic*, July 16, 2013.

“Has U.S. Started an Internet War?,” *CNN*, June 18, 2013.

“Before Prosecuting, Investigate the Government,” *New York Times Room for Debate Blog*, June 11, 2013.

“You Have No Control Over Security on the Feudal Internet,” *Harvard Business Review*, June 6, 2013.

“What We Don’t Know About Spying on Citizens: Scarier Than What We Know,” *The Atlantic*, June 6, 2013.

“The FBI’s New Wiretapping Plan Is Great News for Criminals,” *Foreign Policy*, May 29, 2013.

“It’s Smart Politics to Exaggerate Terrorist Threats,” *CNN*, May 20, 2013.

“Will Giving the Internet Eyes and Ears Mean the End of Privacy?,” *The Guardian*, May 16, 2013.

“Transparency and Accountability Don’t Hurt Security—They’re Crucial to It,” *The Atlantic*, May 8, 2013.

“Why FBI and CIA Didn’t Connect the Dots,” *CNN*, May 2, 2013.

“Do You Want the Government Buying Your Data From Corporations?,” *The Atlantic*, April 30, 2013.

“The Boston Marathon Bombing: Keep Calm and Carry On,” *The Atlantic*, April 15, 2013.

“IT for Oppression,” *IEEE Security & Privacy*, March/April 2013.

“On Security Awareness Training,” *Dark Reading*, March 19, 2013.

“The Internet Is a Surveillance State,” *CNN*, March 16, 2013.

Bruce Schneier CV: Published Articles**26**

“Rhetoric of Cyber War Breeds Fear—and More Cyber War,” *The Irish Times*, March 14, 2013.

“Our Security Models Will Never Work—No Matter What We Do,” *Wired*, March 14, 2013.

“Danger Lurks in Growing New Internet Nationalism,” *MIT Technology Review*, March 11, 2013.

“Take Stop-and-Scan with a Grain of Salt,” *New York Daily News*, March 3, 2013.

“The Court of Public Opinion Is About Mob Justice and Reputation as Revenge,” *Wired*, February 26, 2013.

“How Secure Is the Papal Election?,” *CNN*, February 21, 2013.

“Trust and Society,” *The Montréal Review*, February 2013.

“Power and the Internet,” *Edge*, January 23, 2013.

“Unsafe Security: A Sociologist Aptly Analyzes our Failures in Top-Down Protection,” *Reason*, January 2013.

“Our New Regimes of Trust,” *The SciTech Lawyer*, Winter/Spring 2013.

“Militarizing Cyberspace Will Do More Harm Than Good,” *The Irish Times*, November 29, 2012.

“When It Comes to Security, We’re Back to Feudalism,” *Wired*, November 26, 2012.

“Lance Armstrong and the Prisoner’s Dilemma of Doping in Professional Sports,” *Wired*, October 26, 2012.

“Fear Pays the Bills, But Accounts Must Be Settled,” *New York Times* Room for Debate blog, October 19, 2012.

“The Importance of Security Engineering,” *IEEE Security & Privacy*, September/October 2012.

“Drawing the Wrong Lessons from Horrific Events,” *CNN*, July 31, 2012.

“Securing Medical Research: A Cybersecurity Point of View,” *Science*, June 22, 2012.

“Debate Club: An International Cyberwar Treaty Is the Only Way to Stem the Threat,” *U.S. News*, June 8, 2012.

“The Vulnerabilities Market and the Future of Security,” *Forbes*, May 30, 2012.

“To Profile or Not to Profile?,” *Sam Harris’s Blog*, May 25, 2012.

“The Trouble with Airport Profiling,” *Forbes*, May 9, 2012.

Bruce Schneier CV: Published Articles**27**

- “Economist Debates: Airport Security,” *The Economist*, March 20, 2012.
- “High-Tech Cheats in a World of Trust,” *New Scientist*, February 27, 2012.
- “The Big Idea: Bruce Schneier,” *Whatever*, February 16, 2012.
- “How Changing Technology Affects Security,” *IEEE Security & Privacy*, March/April 2012.
- “Detecting Cheaters,” *IEEE Security & Privacy*, March/April 2011.
- “Why Terror Alert Codes Never Made Sense,” *CNN*, January 28, 2011.
- “Whitelisting and Blacklisting,” *Information Security*, January 2011.
- “It Will Soon Be Too Late to Stop the Cyberwars,” *Financial Times*, December 2, 2010.
- “Why the TSA Can’t Back Down,” *The Atlantic*, December 2, 2010.
- “Close the Washington Monument,” *The New York Daily News*, December 2, 2010.
- “The Dangers of a Software Monoculture,” *Information Security Magazine*, November 2010.
- “A Waste of Money and Time,” *New York Times Room for Debate Blog*, November 23, 2010.
- “The Plan to Quarantine Infected Computers,” *Forbes*, November 11, 2010.
- “When to Change Passwords,” *Dark Reading*, November 10, 2010.
- “The Difficulty of Surveillance Crowdsourcing,” *Threatpost*, November 8, 2010.
- “The Story Behind The Stuxnet Virus,” *Forbes*, October 7, 2010.
- “Web Snooping Is a Dangerous Move,” *CNN*, September 29, 2010.
- “Should Enterprises Give In to IT Consumerization at the Expense of Security?,” *Information Security*, September 2010.
- “Data Privacy: The Facts of Life,” *The Irish Times*, August 27, 2010.
- “A Taxonomy of Social Networking Data,” *IEEE Security & Privacy*, July/August 2010.
- “3 Reasons to Kill the Internet Kill Switch Idea,” *AOL News*, July 9, 2010.
- “Threat of ‘Cyberwar’ Has Been Hugely Hyped,” *CNN*, July 7, 2010.
- “The Failure of Cryptography to Secure Modern Networks,” *Dark Reading*, June 30, 2010.
- “Weighing the Risk of Hiring Hackers,” *Information Security*, June 2010.

“The Internet: Anonymous Forever,” *Forbes, Information Security*, May 12, 2010.

“Worst-Case Thinking Makes Us Nuts, Not Safe,” *CNN*, May 12, 2010.

“Where Are All the Terrorist Attacks?,” *AOL News*, May 4, 2010.

“Focus on the Threat,” *New York Times Room for Debate Blog*, May 3, 2010.

“The Meaning of Trust,” *The Guardian*, April 16, 2010.

“Scanners, Sensors are Wrong Way to Secure the Subway,” *Daily News*, April 7, 2010.

“Google And Facebook’s Privacy Illusion,” *Forbes*, April 6, 2010.

“Should the Government Stop Outsourcing Code Development?,” *Information Security*, March 2010.

“Spy Cameras Won’t Make Us Safer,” *CNN*, February 25, 2010.

“Security and Function Creep,” *IEEE Security & Privacy*, January/February 2010.

“U.S. Enables Chinese Hacking of Google,” *CNN* and *Ethiopian Review*, January 23, 2010.

“Fixing Intelligence Failures,” *San Francisco Chronicle*, January 15, 2010.

“Stop the Panic on Air Security,” *CNN*, January 7, 2010.

“Our Reaction Is the Real Security Failure,” *AOL News*, January 7, 2010.

“Fixing a Security Problem Isn’t Always the Right Answer,” *Threatpost*, January 5, 2010.

“Profiling Makes Us Less Safe,” *New York Times Room for Debate Blog*, January 4, 2010.

“Is Aviation Security Mostly for Show?,” *CNN*, December 29, 2009.

“Cold War Encryption is Unrealistic in Today’s Trenches,” *The Japan Times* and *Wired News*, December 23, 2009.

“Virus and Protocol Scares Happen Every Day—But Don’t Let Them Worry You,” *The Guardian*, December 9, 2009.

“Nature’s Fears Extend to Online Behavior,” *The Japan Times* and *Dark Reading*, November 18, 2009.

“News Media Strategies for Survival for Journalists,” *Twin Cities Daily Planet*, November 14, 2009.

“Reputation is Everything in IT Security,” *The Guardian*, November 11, 2009.

“Is Antivirus Dead?,” *Information Security*, November 2009.

“Beyond Security Theater,” *New Internationalist*, November 2009.

“‘Zero Tolerance’ Really Means Zero Discretion,” *MPR NewsQ*, November 4, 2009.

“Why Framing Your Enemies Is Now Virtually Child’s Play,” *The Guardian*, October 15, 2009.

“The Difficulty of Un-Authentication,” *Threatpost*, September 28, 2009.

“The Battle Is On Against Facebook and Co to Regain Control of Our Files,” *The Guardian*, September 9, 2009.

“Is Perfect Access Control Possible?,” *Information Security*, September 2009.

“Offhand but On Record,” *The Japan Times*, August 19, 2009.

“Lockpicking and the Internet,” *Dark Reading*, August 10, 2009.

“The Value of Self-Enforcing Protocols,” *Threatpost*, August 10, 2009.

“People Understand Risks—But Do Security Staff Understand People?,” *The Guardian*, *The Sydney Morning Herald*, and *The Age*, August 5, 2009.

“Technology Shouldn’t Give Big Brother a Head Start,” *MPR News Q*, July 31, 2009.

“Protect Your Laptop Data From Everyone, Even Yourself,” *Wired News*, July 15, 2009.

“Facebook Should Compete on Privacy, Not Hide It Away,” *The Guardian*, July 15, 2009.

“So-called Cyberattack Was Overblown,” *MPR News Q* and *ITWire*, July 13, 2009.

“Security, Group Size, and the Human Brain,” *IEEE Security & Privacy*, July/August 2009.

“Clear Common Sense for Takeoff: How the TSA Can Make Airport Security Work for Passengers Again,” *New York Daily News*, June 24, 2009.

“Raising the Cost of Paperwork Errors Will Improve Accuracy,” *The Guardian* and *Gulf Times*, June 24, 2009.

“How Science Fiction Writers Can Help, or Hurt, Homeland Security,” *Wired News*, June 18, 2009.

“Be Careful When You Come to Put Your Trust in the Clouds,” *The Guardian* and *The Japan Times*, June 4, 2009.

“Coordinate, But Distribute Responsibility,” *NYTimes.com*, May 29, 2009.

“We Shouldn’t Poison Our Minds with Fear of Bioterrorism,” *The Guardian*, May 14, 2009.

“Should We Have an Expectation of Online Privacy?,” *Information Security*, May 2009.

“Do You Know Where Your Data Are?,” *The Wall Street Journal*, April 28, 2009.

“How the Great Conficker Panic Hacked into Human Credulity,” *The Guardian* and *Gulf Times*, April 23, 2009.

“An Enterprising Criminal Has Spotted a Gap in the Market,” *The Guardian*, April 2, 2009.

“Who Should Be in Charge of Cybersecurity?,” *The Wall Street Journal*, March 31, 2009.

“It’s Time to Drop the ‘Expectation of Privacy’ Test,” *Wired News*, March 26, 2009.

“Blaming The User Is Easy—But It’s Better to Bypass Them Altogether,” *The Guardian*, March 12, 2009.

“The Kindness of Strangers,” *The Wall Street Journal*, March 12, 2009.

“Privacy in the Age of Persistence,” *BBC News*, February 26, 2009.

“How Perverse Incentives Drive Bad Security Decisions,” *Wired News*, February 26, 2009.

“The Secret Question Is: Why Do IT Systems Use Insecure Passwords?,” *The Guardian*, February 19, 2009.

“Thwarting an Internal Hacker,” *The Wall Street Journal*, February 16, 2009.

“Terrorists May Use Google Earth, But Fear Is No Reason to Ban It,” *The Guardian*, *The Hindu*, *Brisbane Times*, and *The Sydney Morning Herald*, January 29, 2009.

“How to Ensure Police Database Accuracy,” *The Wall Street Journal*, January 27, 2009.

“Architecture of Privacy,” *IEEE Security & Privacy*, Jan/Feb 2009.

“State Data Breach Notification Laws: Have They Helped?,” *Information Security*, Jan 2009.

“Why Technology Won’t Prevent Identity Theft,” *The Wall Street Journal*, January 9, 2009.

“Tigers Use Scent, Birds Use Calls—Biometrics Are Just Animal Instinct,” *The Guardian*, January 8, 2009.

“How to Prevent Digital Snooping,” *The Wall Street Journal*, December 9, 2008.

“When You Lose a Piece of Kit, the Real Loss Is The Data It Contains,” *The Guardian* and *The Hindu*, December 4, 2008.

“Why Obama Should Keep His BlackBerry—But Won’t,” *The Wall Street Journal*, November 21, 2008.

“America’s Next Top Hash Function Begins,” *Wired News*, November 19, 2008.

“Passwords Are Not Broken, but How We Choose them Sure Is,” *The Guardian* and *The Hindu*, November 13, 2008.

“CRB Checking,” Schneier on Security, November 3, 2008.

“Time to Show Bottle and Tackle the Real Issues,” *The Guardian*, October 23, 2008.

“Quantum Cryptography: As Awesome As It Is Pointless,” *Wired News*, October 16, 2008.

“Why Society Should Pay the True Costs of Security,” *The Guardian*, October 2, 2008.

“The Seven Habits of Highly Ineffective Terrorists,” *Wired News*, October 1, 2008.

“Does Risk Management Make Sense?,” *Information Security Magazine*, October 2008.

“Airport Pasta-Sauce Interdiction Considered Harmful,” *Wired News*, September 18, 2008.

“A Fetishistic Approach to Security Is a Perverse Way to Keep Us Safe,” *The Guardian*, September 4, 2008.

“How to Create the Perfect Fake Identity,” *Wired News*, September 4, 2008.

“Security ROI: Fact or Fiction?,” *CSO Magazine*, September 2, 2008.

“Here Comes Here Comes Everybody,” *IEEE Spectrum*, September 2008.

“The TSA’s Useless Photo ID Rules,” *Los Angeles Times*, August 28, 2008.

“Boston Court’s Meddling With ‘Full Disclosure’ Is Unwelcome,” *Wired News*, August 21, 2008.

“The Problem Is Information Insecurity,” *Security Watch*, August 10, 2008.

“Memo to Next President: How to Get Cybersecurity Right,” *Wired News*, August 7, 2008.

“Why Being Open about Security Makes Us All Safer in the Long Run,” *The Guardian*, August 7, 2008.

“How the Human Brain Buys Security,” *IEEE Security and Privacy*, Jul/Aug 2008.

“Lesson From the DNS Bug: Patching Isn’t Enough,” *Wired News*, July 23, 2008.

“Software Makers Should Take Responsibility,” *The Guardian*, July 17, 2008.

“How a Classic Man-in-the-Middle Attack Saved Colombian Hostages,” *Wired News*, July 10, 2008.

“Chinese Cyberattacks: Myth or Menace?,” *Information Security Magazine*, July 2008.

“I’ve Seen the Future, and It Has a Kill Switch,” *Wired News*, June 30, 2008.

“CCTV Doesn’t Keep Us Safe, Yet the Cameras Are Everywhere,” *The Guardian*, June 26, 2008.

“The Truth About Chinese Hackers,” *Discovery Technology*, June 19, 2008.

“The Pros and Cons of Lifelock,” *Wired News*, June 12, 2008.

“Are Photographers Really a Threat?,” *The Guardian*, June 4, 2008.

“Why Do We Accept Signatures by Fax?,” *Wired News*, May 29, 2008.

“How to Sell Security,” *CIO*, May 26, 2008.

“Our Data, Ourselves,” *Wired News*, May 15, 2008.

“Crossing Borders with Laptops and PDAs,” *The Guardian*, May 15, 2008.

“America’s Dilemma: Close Security Holes, or Exploit Them Ourselves,” *Wired News*, May 1, 2008.

“The Ethics of Vulnerability Research,” *Information Security Magazine*, May 2008.

“Prediction: RSA Conference Will Shrink Like a Punctured Balloon,” *Wired News*, April 17, 2008.

“Secret Questions Blow a Hole in Security,” *ComputerWeekly*, April 4, 2008.

“The Difference Between Feeling and Reality in Security,” *Wired News*, April 3, 2008.

“Inside the Twisted Mind of the Security Professional,” *Wired News*, March 20, 2008.

“Census of Cyberspace Censoring,” *Nature*, March 13, 2008.

“The Myth of the ‘Transparent Society,’” *Wired News*, March 6, 2008.

“Consolidation: Plague or Progress,” *Information Security Magazine*, March 2008.

“Security at What Cost?,” *Minneapolis Star Tribune*, February 23, 2008.

“When the Internet Is My Hard Drive, Should I Trust Third Parties?,” *Wired News*, February 21, 2008.

“Driver’s Licenses for Immigrants: Denying Licenses Makes Us Less Safe,” *Detroit Free Press*, February 7, 2008.

“With iPhone, ‘Security’ Is Code for ‘Control,’” *Wired News*, February 7, 2008.

“What Our Top Spy Doesn’t Get: Security and Privacy Aren’t Opposites,” *Wired News*, January 24, 2008.

“Steal This Wi-Fi,” *Wired News*, January 10, 2008.

“Why ‘Anonymous’ Data Sometimes Isn’t,” *Wired News*, December 13, 2007.

“Caution: Turbulence Ahead,” *Information Security Magazine*, December 2007.

“The Death of the Security Industry,” *IEEE Security and Privacy*, Nov/Dec 2007.

“How Does Bruce Schneier Protect His Laptop Data? With His Fists — and PGP,” *Wired News*, November 29, 2007.

“Did NSA Put a Secret Backdoor in New Encryption Standard?,” *Wired News*, November 15, 2007.

“Cyberwar: Myth or Reality?,” *Information Security Magazine*, November 2007.

“How We Won the War on Thai Chili Sauce,” *Wired News*, November 1, 2007.

“Economics, Not Apathy, Exposes Chemical Plants To Danger,” *Wired News*, October 18, 2007.

“Paying the Cost of Insecure Software [PDF],” *OutlookBusiness*, October 5, 2007.

“Gathering ‘Storm’ Superworm Poses Grave Threat to PC Nets,” *Wired News*, October 4, 2007.

“Lesson From Tor Hack: Anonymity and Privacy Aren’t the Same,” *Wired News*, September 20, 2007.

“NBA Ref Scandal Warns of Single Points of Failure,” *Wired News*, September 6, 2007.

“Home Users: A Public Health Problem?,” *Information Security Magazine*, September 2007.

“Time to Close Gaps in Emergency Communications,” *Wired News*, August 23, 2007.

“E-Voting Certification Gets Security Completely Backward,” *Wired News*, August 9, 2007.

“Interview with Kip Hawley,” *Schneier on Security*, August 3, 2007.

“Disaster Planning Is Critical, but Pick a Reasonable Disaster,” *Wired News*, July 26, 2007.

- “The Evolutionary Brain Glitch That Makes Terrorism Fail,” *Wired News*, July 12, 2007.
- “Strong Laws, Smart Tech Can Stop Abusive ‘Data Reuse,’” *Wired News*, June 28, 2007.
- “Portrait of the Modern Terrorist as an Idiot,” *Wired News*, June 14, 2007.
- “Don’t Look a Leopard in the Eye, and Other Security Advice,” *Wired News*, May 31, 2007.
- “Virginia Tech Lesson: Rare Risks Breed Irrational Responses,” *Wired News*, May 17, 2007.
- “Will REAL ID Actually Make Us Safer?,” *Testimony before the Senate Judiciary Committee*, May 8, 2007.
- “Nonsecurity Considerations in Security Decisions,” *IEEE Computers and Security*, May 6, 2007.
- “Do We Really Need a Security Industry?,” *Wired News*, May 3, 2007.
- “Psychology of Security,” *Communications of the ACM*, May 2007.
- “Is Big Brother a Big Deal?,” *Information Security Magazine*, May 2007.
- “How Security Companies Sucker Us With Lemons,” *Wired News*, April 19, 2007.
- “Vigilantism Is a Poor Response to Cyberattack,” *Wired News*, April 5, 2007.
- “How to Not Catch Terrorists,” *Forbes*, March 26, 2007.
- “Why the Human Brain Is a Poor Judge of Risk,” *Wired News*, March 22, 2007.
- “The Problem With Copycat Cops,” *Wired News*, March 8, 2007.
- “Real-ID: Costs and Benefits,” *The Bulletin of the Atomic Scientists*, March 4, 2007.
- “Is Penetration Testing Worth It?,” *Information Security Magazine*, March 2007.
- “Privatizing the Police Puts Us at Greater Risk,” *Minneapolis Star Tribune*, February 27, 2007.
- “Why Smart Cops Do Dumb Things,” *Wired News*, February 22, 2007.
- “Why Vista’s DRM Is Bad For You,” *Forbes*, February 12, 2007.
- “An American Idol for Crypto Geeks,” *Wired News*, February 8, 2007.
- “The Psychology of Security,” February 7, 2007.
- “In Praise of Security Theater,” *Wired News*, January 25, 2007.
- “Solving Identity Theft,” *Forbes*, January 22, 2007.

“Life in the Fast Lane,” *The New York Times* and *The Mercury News*, January 21, 2007.

“Camera Phones vs. Crime: Now We’re Talking,” *New York Daily News*, January 19, 2007.

“On Police Security Cameras,” *San Francisco Chronicle* and *Arizona Daily Star*, January 16, 2007.

“Secure Passwords Keep You Safer,” *Wired News*, January 15, 2007.

“They’re Watching,” *Forbes*, January 8, 2007.

“Does Secrecy Help Protect Personal Information?,” *Information Security*, January 2007.

“Information Security and Externalities,” *ENISA Quarterly*, January 2007.

“Schneier: Full Disclosure of Security Vulnerabilities a ‘Damned Good Idea,’” *CSO Online*, January 2007.

“MySpace Passwords Aren’t So Dumb,” *Wired News*, December 14, 2006.

“Why Spam Won’t Go Away,” *Forbes*, December 12, 2006.

“My Data, Your Machine,” *Wired News*, November 30, 2006.

“Vote Early, Vote Often,” *Wired News*, November 16, 2006.

“Did Your Vote Get Counted?,” *Forbes*, November 13, 2006.

“The Boarding Pass Brouhaha,” *Wired News*, November 2, 2006.

“Do Federal Security Regulations Help?,” *Information Security Magazine*, November 2006.

“The Architecture of Security,” *Wired News*, October 19, 2006.

“Casual Conversation, R.I.P.,” *Forbes*, October 18, 2006.

“Why Everyone Must Be Screened,” *Wired News*, October 5, 2006.

“Lessons From the Facebook Riots,” *Wired News*, September 21, 2006.

“The ID Chip You Don’t Want in Your Passport,” *Washington Post*, September 16, 2006.

“Quickest Patch Ever,” *Wired News*, September 7, 2006.

“Is There Strategic Software?,” *Information Security Magazine*, September 2006.

“Refuse to be Terrorized,” *Wired News*, August 24, 2006.

“Focus on Terrorists, Not Tactics,” *Minneapolis Star Tribune*, August 13, 2006.

- “Drugs: Sports’ Prisoner’s Dilemma,” *Wired News*, August 10, 2006.
- “How Bot Those Nets?,” *Wired News*, July 27, 2006.
- “Google’s Click-Fraud Crackdown,” *Wired News*, July 13, 2006.
- “Are Security Certifications Valuable?,” *Information Security Magazine*, July 2006.
- “It’s the Economy, Stupid,” *Wired News*, June 29, 2006.
- “The Scariest Terror Threat of All,” *Wired News*, June 15, 2006.
- “Make Vendors Liable for Bugs,” *Wired News*, June 1, 2006.
- “We’re Giving Up Privacy and Getting Little in Return,” *Minneapolis Star Tribune*, May 31, 2006.
- “The Eternal Value of Privacy,” *Wired News*, May 18, 2006.
- “Everyone Wants to ‘Own’ Your PC,” *Wired News*, May 4, 2006.
- “The Anti-ID-Theft Bill That Isn’t,” *Wired News*, April 20, 2006.
- “Why VOIP Needs Crypto,” *Wired News*, April 6, 2006.
- “Is User Education Working?,” *Information Security Magazine*, April 2006.
- “Let Computers Screen Air Baggage,” *Wired News*, March 23, 2006.
- “Why Data Mining Won’t Stop Terror,” *Wired News*, March 9, 2006.
- “Your Vanishing Privacy,” *Minneapolis Star Tribune*, March 5, 2006.
- “U.S. Ports Raise Proxy Problem,” *Wired News*, February 23, 2006.
- “Security in the Cloud (Feb 06),” *Network World*, February 15, 2006.
- “Fighting Fat-Wallet Syndrome,” *Wired News*, February 9, 2006.
- “Big Risks Come in Small Packages,” *Wired News*, January 26, 2006.
- “Anonymity Won’t Kill the Internet,” *Wired News*, January 12, 2006.
- “Unchecked Presidential Power,” *Minneapolis Star Tribune*, December 20, 2005.
- “Uncle Sam is Listening,” *Salon*, December 20, 2005.
- “Hold the Photons!,” *Wired News*, December 15, 2005.
- “The Hackers are Coming!,” *Utility Automation & Engineering T&D*, December 13, 2005.

- “Airline Security a Waste of Cash,” *Wired News*, December 1, 2005.
- “The Zotob Storm,” *IEEE Security and Privacy*, Nov/Dec 2005.
- “The Erosion of Freedom,” *Minneapolis Star Tribune*, November 21, 2005.
- “Real Story of the Rogue Rootkit,” *Wired News*, November 17, 2005.
- “Fatal Flaw Weakens RFID Passports,” *Wired News*, November 3, 2005.
- “Sue Companies, Not Coders,” *Wired News*, October 20, 2005.
- “A Real Remedy for Phishers,” *Wired News*, October 6, 2005.
- “University Networks and Data Security,” *IEEE Security and Privacy*, Sep/Oct 2005.
- “A Sci-Fi Future Awaits the Court,” *Wired News*, September 22, 2005.
- “Toward a Truly Safer Nation,” *Minneapolis Star Tribune*, September 11, 2005.
- “Terrorists Don’t Do Movie Plots,” *Wired News*, September 8, 2005.
- “Make Businesses Pay in Credit Card Scam,” *New York Daily News*, June 23, 2005.
- “Attack Trends: 2004 and 2005,” *Queue*, June 2, 2005.
- “Risks of Third-Party Data,” *Communications of the ACM*, May 2005.
- “Two-Factor Authentication: Too Little, Too Late,” *Communications of the ACM*, April 2005.
- “Digital Information Rights Need Tech-Savvy Courts,” *eWeek*, February 14, 2005.
- “The Curse of the Secret Question,” *Computerworld*, February 9, 2005.
- “Authentication and Expiration,” *IEEE Security and Privacy*, Jan/Feb 2005.
- “Who says safe computing must remain a pipe dream?,” *CNET News.com*, December 9, 2004.
- “Airport Security and Metal Knives,” *The Sydney Morning Herald*, November 30, 2004.
- “Desktop Google Finds Holes,” *eWeek*, November 29, 2004.
- “Profile: ‘hinky,’” *Boston Globe*, November 24, 2004.
- “Why is it so hard to run an honest election?,” *OpenDemocracy*, November 24, 2004.
- “Getting Out the Vote,” *San Francisco Chronicle*, October 31, 2004.
- “Information Security: How Liable Should Vendors Be?,” *Computerworld*, October 28, 2004.

- “The Security of Checks and Balances,” *The Sydney Morning Herald*, October 26, 2004.
- “Outside View: Security at the World Series,” *UPI*, October 22, 2004.
- “Bigger Brother,” *The Baltimore Sun*, October 4, 2004.
- “Does Big Brother want to watch?,” *International Herald Tribune*, October 4, 2004.
- “Do Terror Alerts Work?,” *The Rake*, October 2004.
- “The Non-Security of Secrecy,” *Communications of the ACM*, October 2004.
- “SIMS: Solution, or Part of the Problem?,” *IEEE Security and Privacy*, Sep/Oct 2004.
- “Saluting the data encryption legacy,” *CNET News.com*, September 27, 2004.
- “Academics locked out by tight visa controls,” *Mercury News*, September 20, 2004.
- “City Cops’ Plate Scanner is a License to Snoop,” *New Haven Register*, September 19, 2004.
- “We Owe Much to DES,” *eWeek*, August 30, 2004.
- “How Long Can the Country Stay Scared?,” *Minneapolis Star Tribune*, August 27, 2004.
- “Olympic Security,” *The Sydney Morning Herald*, August 26, 2004.
- “U.S. ‘No-Fly’ List Curtails Liberties,” *Newsday*, August 25, 2004.
- “An Easy Path for Terrorists,” *Boston Globe*, August 24, 2004.
- “Cryptanalysis of MD5 and SHA: Time for a New Standard,” *Computerworld*, August 19, 2004.
- “BOB on Board,” *The Sydney Morning Herald*, August 2, 2004.
- “Customers, Passwords, and Web Sites,” *IEEE Security and Privacy*, Jul/Aug 2004.
- “Security, Houston-Style,” *The Sydney Morning Herald*, July 30, 2004.
- “US-VISIT Is No Bargain,” *eWeek*, July 6, 2004.
- “Insider Risks in Elections,” *Communications of the ACM*, July 2004.
- “Unchecked Police And Military Power Is A Security Threat,” *Minneapolis Star Tribune*, June 24, 2004.
- “CLEARly Muddying the Fight Against Terror,” *News.com*, June 16, 2004.
- “The Witty Worm: A New Chapter in Malware,” *Computerworld*, June 2, 2004.
- “Security and Compliance,” *IEEE Security and Privacy*, May/Jun 2004.

- “Microsoft’s Actions Speak Louder Than Words,” *Network World*, May 31, 2004.
- “Curb Electronic Surveillance Abuses,” *Newsday*, May 10, 2004.
- “We Are All Security Customers,” *CNET News.com*, May 4, 2004.
- “Terrorist Threats and Political Gains,” *Counterpunch*, April 27, 2004.
- “Hacking the Business Climate for Network Security,” *IEEE Computer*, April 2004.
- “A National ID Card Wouldn’t Make Us Safer,” *Minneapolis Star Tribune*, April 1, 2004.
- “Cyber Underwriters Lab?,” *Communications of the ACM*, April 2004.
- “America’s Flimsy Fortress,” *Wired Magazine*, March 2004.
- “IDs and the illusion of security,” *San Francisco Chronicle*, February 3, 2004.
- “Risks of PKI: Electronic Commerce,” *Communications of the ACM*, February 2004.
- “Voting Security,” *IEEE Security and Privacy*, Jan/Feb 2004.
- “Slouching Towards Big Brother,” *CNET News.com*, January 30, 2004.
- “Homeland Insecurity,” *Salon.com*, January 19, 2004.
- “Fingerprinting Visitors Won’t Offer Security,” *Newsday*, January 14, 2004.
- “Risks of PKI: Secure E-Mail,” *Communications of the ACM*, January 2004.
- “Better Get Used to Routine Loss of Personal Privacy,” *Minneapolis Star Tribune*, December 21, 2003.
- “Are You Sophisticated Enough to Recognize an Internet Scam?,” *Mercury News*, December 19, 2003.
- “Blaster and the Great Blackout,” *Salon.com*, December 16, 2003.
- “Internet Worms and Critical Infrastructure,” *CNET News.com*, December 9, 2003.
- “Airplane Hackers,” *IEEE Security and Privacy*, Nov/Dec 2003.
- “Festung Amerika,” *Financial Times Deutschland*, November 11, 2003.
- “Liability Changes Everything,” *Heise Security*, November 2003.
- “Terror Profiles by Computers Are Ineffective,” *Newsday*, October 21, 2003.
- “Fixing intelligence,” *UPI*, October 14, 2003.
- “CyberInsecurity: The Cost of Monopoly,” *Computer & Communications Industry Association Report*, September 24, 2003.

“Voting and Technology: Who Gets to Count Your Vote?,” *Communications of the ACM*, August 2003.

“The Speed of Security,” *IEEE Security and Privacy*, Jul/Aug 2003.

“Walls Don’t Work in Cyberspace,” *Wired Magazine*, June 2003.

“Guilty Until Proven Innocent?,” *IEEE Security and Privacy*, May/Jun 2003.

“Locks and Full Disclosure,” *IEEE Security and Privacy*, Mar/Apr 2003.

“American Cyberspace: Can We Fend Off Attackers?,” *Mercury News*, March 7, 2003.

“Secrecy and Security,” *SF Chronicle*, March 2, 2003.

“We Are All Security Consumers,” *IEEE Security and Privacy*, Jan/Feb 2003.

“Trust, but Verify, Microsoft’s Pledge,” *CNET News.com*, January 18, 2002.

“The Case for Outsourcing Security,” *IEEE Computer Magazine*, 2002.

“Foreword,” *Security Engineering* by Ross Anderson, May 2001.

“Body of Secrets by James Bamford (Review),” *Salon.com*, April 2001.

“Insurance and the Computer Industry,” *Communications of the ACM*, March 2001.

“The Insurance Takeover,” *Information Security Magazine*, February 2001.

“The Third Wave of Network Attacks,” *ZDNet*, October 3, 2000.

“The Fallacy of Trusted Client Software,” *Information Security Magazine*, August 2000.

“The Process of Security,” *Information Security Magazine*, April 2000.

“1999 Crypto Year-in-Review,” *Information Security Magazine*, December 1999.

“DVD Encryption Broken,” *ZDNet*, November 1999.

“Why Computers are Insecure,” *Computerworld*, November 1999.

“A Plea for Simplicity,” *Information Security Magazine*, November 1999.

“Risks of Relying on Cryptography,” *Communications of the ACM*, October 1999.

“The Trojan Horse Race,” *Communications of the ACM*, September 1999.

“International Cryptography,” *Information Security Magazine*, September 1999.

“Web-Based Encrypted E-Mail,” *ZDNet*, August 1999.

“NIST AES News,” *ZDNet*, August 1999.

“Biometrics: Uses and Abuses,” *Communications of the ACM*, August 1999.

“Cryptography: The Importance of Not Being Different,” *IEEE Security and Privacy*, March 1999.

“Why the Worst Cryptography is in the Systems that Pass Initial Analysis,” *Information Security Magazine*, March 1999.

“Intel’s Processor ID,” *ZDNet*, January 26, 1999.

“How to Evaluate Security Technology,” *Computer Security Journal*, 1999.

“1998 Crypto Year-in-Review,” *Information Security Magazine*, December 1998.

“Key Recovery,” *Information Security Magazine*, October 1998.

“Security Pitfalls in Cryptography,” *Schneier on Security*, 1998.

“Click here to bring down the Internet,” *Schneier on Security*, 1998.

“Cryptography, Security, and the Future,” *Communications of the ACM*, January 1997.

“Why Cryptography is Harder than it Looks,” *Schneier on Security*, 1997.

Patents

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for educational testing,” U.S. Patent 8,725,060, May 13, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers,” U.S. Patent 8,712,920, April 29, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 8,700,481, April 15, 2014.

J.S. Walker, B. Schneier, M.M Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, “Method and apparatus for promoting the selection and use of a transaction card,” U.S. Patent 8,632,005, January 21, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce,” U.S. Patent 8,626,667, January 7, 2014.

B. Schneier, J.S. Walker, J.A. Jorasch, G.M Gelman, “System and method for securing electronic games,” U.S. Patent 8,608,558, December 17, 2013.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 8,549,310, October 1, 2013.

J.S. Walker, B. Schneier, “Method and apparatus for executing cryptographically-enabled letters of credit,” U.S. Patent 8,355,991, January 15, 2013.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce,” U.S. Patent 8,326,765, December 4, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and device for generating a single-use financial account number,” U.S. Patent 8,315,948, November 20, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 8,250,369, August 21, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers,” U.S. Patent 8,135,650, March 13, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 8,086,653, December 27, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for educational testing,” U.S. Patent 8,086,167, December 27, 2011.

J.S. Walker, T.S. Case, J.A. Jorasch, B. Schneier, “Conditional purchase offer management system,” U.S. Patent 8,082,221, December 20, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 8,082,180, December 20, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, “Method and apparatus for verifying secure document timestamping,” U.S. Patent RE42,893, November 1, 2011.

J.S. Walker, B. Schneier, “Method and apparatus for executing cryptographically-enabled letters of credit,” U.S. Patent 7,991,698, August 2, 2011.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, “Method and apparatus for promoting the selection and use of a transaction card,” U.S. Patent 7,988,044, August 2, 2011.

B. Schneier, A.H. Gross, J.D. Callas, “Method and system for dynamic network intrusion monitoring, detection and response,” U.S. Patent 7,895,641, February 22, 2011.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 7,887,405, February 15, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, “Method and apparatus for verifying secure document timestamping,” U.S. Patent RE42,018, December 28, 2010.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 7,853,529, December 14, 2010.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 7,844,550, November 30, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, “Method and apparatus for verifying secure document timestamping,” U.S. Patent RE41,960, November 23, 2010.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, “Method and apparatus for promoting the selection and use of a transaction card,” U.S. Patent 7,806,320, October 5, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 7,664,672, February 16, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 7,620,619, November 17, 2009.

B. Schneier, J.S. Walker, J.A. Jorasch, G.M. Gelman, “System and method for securing electronic games,” U.S. Patent 7,524,245, April 28, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically assisted commercial network system designed to facilitate and support expert-based commerce,” U.S. Patent 7,523,045, April 21, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for educational testing,” U.S. Patent 7,483,670, January 27, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a commercial network system designed to facilitate buyer-driven conditional purchase offers,” U.S. Patent 7,472,074, December 30, 2008.

B. Schneier, J.S. Walker, J.A. Jorasch, “Methods and apparatus for awarding prizes based on authentication of computer generated outcomes using coupons,” U.S. Patent 7,362,862, April 22, 2008.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 7,303,468, December 4, 2007.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 7,285,045, October 23, 2007.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 7,177,835, February 13, 2007.

B. Schneier, A.H. Gross, J.D. Callas, “Method and system for dynamic network intrusion monitoring, detection and response,” U.S. Patent 7,159,237, January 2, 2007.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, “Method and apparatus for promoting the selection and use of a transaction card,” U.S. Patent 7,090,123, August 15, 2006.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 7,008,318, March 7, 2006.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, “Method and apparatus for verifying secure document timestamping,” U.S. Patent 6,959,387, October 25, 2005.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 6,942,570, September 13, 2005.

J.S. Walker, B. Schneier, “Method and apparatus for remote gaming,” U.S. Patent 6,935,952, August 30, 2005.

J.S. Walker, B. Schneier, “Method and apparatus for executing cryptographically-enabled letters of credit,” U.S. Patent 6,904,418, June 7, 2005.

J.S. Walker, B. Schneier, J.A. Jorasch, A.S. Van Luchene, “Method and apparatus for securing a computer-based game of chance,” U.S. Patent 6,790,139, September 14, 2004.

J.S. Walker, B. Schneier, M.M. Fincham, “Device and method for promoting the selection and use of a transaction card,” U.S. Patent 6,739,505, May 25, 2004.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 6,607,439, August 19, 2003.

J.S. Walker, B. Schneier, “Secure improved remote gaming system,” U.S. Patent 6,527,638, March 4, 2003.

J.S. Walker, S.K. Jindal, B. Schneier, T. Weir-Jones, “System and method for managing third-party input to a conditional purchase offer (CPO),” U.S. Patent 6,484,153, November 19, 2002.

J.S. Walker, B. Schneier, “Method and apparatus for executing cryptographically-enabled letters of credit,” U.S. Patent 6,477,513, November 5, 2002.

B. Schneier, J.S. Walker, J.A. Jorasch, “Method and apparatus for securing electronic games,” U.S. Patent 6,450,885, September 17, 2002.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 6,402,614, June 11, 2002.

S.T. Ansell, A.R. Cherenson, M.E. Paley, S.B. Katz, J.M. Kelsey, Jr., B. Schneier, “Copy security for portable music players,” U.S. Patent 6,367,019, April 2, 2002.

J.S. Walker, T.M. Sparico, B. Schneier, “Conditional purchase offer management system for telephone calls,” U.S. Patent 6,345,090, February 5, 2002.

J.S. Walker, B. Schneier, M. Mik, “Device and method for promoting the selection and use of a credit card,” U.S. Patent 6,325,284, December 4, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 6,289,453, September 11, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 6,282,648, August 28, 2001.

B. Schneier, J.S. Walker, J.A. Jorasch, “Method and apparatus for securing electronic games,” U.S. Patent 6,264,557, July 24, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure document timestamping,” U.S. Patent 6,263,438, July 17, 2001.

J.S. Walker, B. Schneier, “Systems and methods for a user to access digital data provided by an on-line server over a data network,” U.S. Patent 6,249,865, June 19, 2001.

J.S. Walker, R.R. Lech, A.S. Van Luchene, T.M. Sparico, J.A. Jorasch, B. Schneier, “Conditional purchase offer management system for event tickets,” U.S. Patent 6,240,396, May 29, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, A.S. Van Luchene, “Method and apparatus for securing a computer-based game of chance,” U.S. Patent 6,203,427, March 20, 2001.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 6,163,771, December 19, 2000.

J.S. Walker, T.M. Sparico, T.S. Case, B. Schneier, “Conditional purchase offer management system for cruises,” U.S. Patent 6,134,534, October 17, 2000.

R. Martinez, B. Schneier, G. Guerin, “Virtual property system,” U.S. Patent 6,119,229, September 12, 2000.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for authenticating a document,” U.S. Patent 6,111,953, August 29, 2000.

B. Schneier, J.S. Walker, J.A. Jorasch, “Method and apparatus for securing electronic games,” U.S. Patent 6,099,408, August 8, 2000.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 6,085,169, July 4, 2000.

J.S. Walker, B. Schneier, “Off-line remote lottery system,” U.S. Patent 6,024,640, February 15, 2000.

B. Schneier, J.M. Kelsey, “Event auditing system,” U.S. Patent 5,978,475, November 2, 1999.

B. Schneier, J.S. Walker, J.A. Jorasch, “Remote-auditing of computer generated outcomes, authenticated billing and access control, and software metering system using cryptographic and other protocols,” U.S. Patent 5,970,143, October 19, 1999.

B. Schneier, J.M. Kelsey, “Digital signature with auditing bits,” U.S. Patent 5,956,404, September 21, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for computer-based educational testing,” U.S. Patent 5,947,747, September 7, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure document timestamping,” U.S. Patent 5,923,763, July 13, 1999.

J.S. Walker, B. Schneier, T.S. Case, “Method and system for establishing and maintaining user-controlled anonymous communications,” U.S. Patent 5,884,272, March 16, 1999.

J.S. Walker, B. Schneier, T.S. Case, “Method and system for facilitating an employment search incorporating user-controlled anonymous communications,” U.S. Patent 5,884,270, March 16, 1999.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 5,871,398, February 16, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce,” U.S. Patent 5,862,223, January 19, 1999.

Schneier; Bruce, “Method and apparatus for analyzing information systems using stored tree database structures,” U.S. Patent 5,850,516, December 15, 1998.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 5,828,751, October 27, 1998.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers,” U.S. Patent 5,794,207, August 11, 1998.

B. Schneier, J.S. Walker, J.A. Jorasch, “Remote-auditing of computer generated outcomes and authenticated billing and access control system using cryptographic and other protocols,” U.S. Patent 5,768,382, June 16, 1998.

J.S. Walker, B. Schneier, “900 number billing and collection system and method for on-line computer services,” U.S. Patent 5,737,414, April 7, 1998.

Published Crypto-Gram Issues

December 15, 2022: Another Event-Related Spyware App, Russian Software Company Pretending to Be American, Failures in Twitter's Two-Factor Authentication System, Successful Hack of Time-Triggered Ethernet, First Review of A Hacker's Mind, Breaking the Zeppelin Ransomware Encryption Scheme, Apple's Device Analytics Can Identify iCloud Users, The US Has a Shortage of Bomb-Sniffing Dogs, Computer Repair Technicians Are Stealing Your Data, Charles V of Spain Secret Code Cracked, Facebook Fined \$276M under GDPR, Sirius XM Software Vulnerability, LastPass Security Breach, Existential Risk and the Fermi Paradox, CAPTCHA, CryWiper Data Wiper Targeting Russian Sites, The Decoupling Principle, Leaked Signing Keys Are Being Used to Sign Malware, Security Vulnerabilities in Eufy Cameras, Hacking Trespass Law, Apple Is Finally Encrypting iCloud Backups, Obligatory ChatGPT Post, Hacking Boston's CharlieCard, Reimagining Democracy

November 15, 2022: New Book: A Hacker's Mind, Hacking Automobile Keyless Entry Systems, Qatar Spyware, Museum Security, Interview with Signal's New President, Adversarial ML Attack that Secretly Gives a Language Model a Point of View, On the Randomness of Automatic Card Shufflers, Australia Increases Fines for Massive Data Breaches, Critical Vulnerability in Open SSL, Apple Only Commits to Patching Latest OS Version, Iran's Digital Surveillance Tools Leaked, NSA on Supply Chain Security, The Conviction of Uber's Chief Security Officer, Using Wi-Fi to See through Walls, Defeating Phishing-Resistant Multifactor Authentication, An Untrustworthy TLS Certificate in Browsers, NSA Over-surveillance, A Digital Red Cross, Upcoming Speaking Engagements

October 15, 2022: Relay Attack against Teslas, Massive Data Breach at Uber, Large-Scale Collection of Cell Phone Data at US Borders, Credit Card Fraud That Bypasses 2FA, Automatic Cheating Detection in Human Racing, Prompt Injection/Extraction Attacks against AI Systems, Leaking Screen Information on Zoom Calls through Reflections in Eyeglasses, Leaking Passwords through the Spellchecker, New Report on IoT Security, Cold War Bugging of Soviet Facilities, Differences in App Security/Privacy Based on Country, Security Vulnerabilities in Covert CIA Websites, Detecting Deepfake Audio by Modeling the Human Acoustic Tract, NSA Employee Charged with Espionage, October Is Cybersecurity Awareness Month, Spyware Maker Intellexa Sued by Journalist, Complex Impersonation Story, Inserting a Backdoor into a Machine-Learning System, Recovering Passwords by Measuring Residual Heat, Digital License Plates, Regulating DAOs, Upcoming Speaking Engagements

September 15, 2022: \$23 Million YouTube Royalties Scam, Remotely Controlling Touchscreens, Zoom Exploit on MacOS, USB "Rubber Ducky" Attack Tool, Hyundai Uses Example Keys for Encryption System, Signal Phone Numbers Exposed in Twilio Hack, Mudge Files Whistleblower Complaint against Twitter, Man-in-the-Middle Phishing Attack, Security and Cheap Complexity, Levels of Assurance for DoD Microelectronics, FTC Sues Data Broker, High-School Graduation Prank Hack, Clever Phishing Scam Uses Legitimate PayPal Messages, Montenegro Is the Victim of a

Cyberattack, The LockBit Ransomware Gang Is Surprisingly Professional, Facebook Has No Idea What Data It Has, Responsible Disclosure for Cryptocurrency Security, New Linux Cryptomining Malware, FBI Seizes Stolen Cryptocurrencies, Weird Fallout from Peiter Zatkó's Twitter Whistleblowing, Upcoming Speaking Engagements

August 15, 2022: San Francisco Police Want Real-Time Access to Private Surveillance Cameras, Facebook Is Now Encrypting Links to Prevent URL Stripping, NSO Group's Pegasus Spyware Used against Thailand Pro-Democracy Activists and Leaders, Russia Creates Malware False-Flag App, Critical Vulnerabilities in GPS Trackers, Apple's Lockdown Mode, Securing Open-Source Software, New UEFI Rootkit, Microsoft Zero-Days Sold and Then Used, Ring Gives Videos to Police without a Warrant or User Consent, Surveillance of Your Car, Drone Deliveries into Prisons, SIKE Broken, NIST's Post-Quantum Cryptography Standards, Hacking Starlink, A Taxonomy of Access Control, Twitter Exposes Personal Information for 5.4 Million Accounts, Upcoming Speaking Engagements

July 15, 2022: M1 Chip Vulnerability, Attacking the Performance of Machine Learning Systems, Tracking People via Bluetooth on Their Phones, Hertzbleed: A New Side-Channel Attack, Hidden Anti-Cryptography Provisions in Internet Anti-Trust Bills, Symbiote Backdoor in Linux, On the Subversion of NIST by the NSA, On the Dangers of Cryptocurrencies and the Uselessness of Blockchain, 2022 Workshop on Economics and Information Security (WEIS), When Security Locks You Out of Everything, Ecuador's Attempt to Resettle Edward Snowden, ZuoRAT Malware Is Targeting Routers, Analyzing the Swiss E-Voting System, NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, Ubiquitous Surveillance by ICE, Apple's Lockdown Mode, Nigerian Prison Break, Security Vulnerabilities in Honda's Keyless Entry System, Post-Roe Privacy, New Browser De-anonymization Technique, Upcoming Speaking Engagements

June 15, 2022: The NSA Says that There are No Known Flaws in NIST's Quantum-Resistant Algorithms, Attacks on Managed Service Providers Expected to Increase, iPhone Malware that Operates Even When the Phone Is Turned Off, Websites that Collect Your Data as You Type, Bluetooth Flaw Allows Remote Unlocking of Digital Locks, The Onion on Google Map Surveillance, Forging Australian Driver's Licenses, The Justice Department Will No Longer Charge Security Researchers with Criminal Hacking, Manipulating Machine-Learning Systems through the Order of the Training Data, Malware-Infested Smart Card Reader, Security and Human Behavior (SHB) 2022, The Limits of Cyber Operations in Wartime, Clever -- and Exploitable -- Windows Zero-Day, Remotely Controlling Touchscreens, Me on Public-Interest Tech, Long Story on the Accused CIA Vault 7 Leaker, Leaking Military Secrets on Gaming Discussion Boards, Smartphones and Civilians in Wartime, Twitter Used Two-Factor Login Details for Ad Targeting, Cryptanalysis of ENCSecurity's Encryption Implementation, Hacking Tesla's Remote Key Cards, Upcoming Speaking Engagements

May 15, 2022: Undetectable Backdoors in Machine-Learning Models, Clever Cryptocurrency Theft, Long Article on NSO Group, Java Cryptography Implementation

Mistake Allows Digital-Signature Forgeries, SMS Phishing Attacks are on the Rise, Zero-Day Vulnerabilities Are on the Rise, Microsoft Issues Report of Russian Cyberattacks against Ukraine, Video Conferencing Apps Sometimes Ignore the Mute Button, Using Pupil Reflection in Smartphone Camera Selfies, New Sophisticated Malware, 15.3 Million Request-Per-Second DDoS Attack, Corporate Involvement in International Cybersecurity Treaties, Apple Mail Now Blocks Email Trackers, ICE Is a Domestic Surveillance Agency, Surveillance by Driverless Car, Upcoming Speaking Engagements

April 15, 2022: US Critical Infrastructure Companies Will Have to Report When They Are Hacked, Breaking RSA through Insufficiently Random Primes, "Change Password", Why Vaccine Cards Are So Easily Forged, Developer Sabotages Open-Source Software Package, White House Warns of Possible Russian Cyberattacks, NASA's Insider Threat Program, Linux Improves Its Random Number Generator, Gus Simmons's Memoir, A Detailed Look at the Conti Ransomware Gang, Stalking with an Apple Watch, Chrome Zero-Day from North Korea, Bypassing Two-Factor Authentication, Wyze Camera Vulnerability, Hackers Using Fake Police Data Requests against Tech Companies, Cyberweapons Arms Manufacturer FinFisher Shuts Down, US Disrupts Russian Botnet, AirTags Are Used for Stalking Far More than Previously Reported, De-anonymizing Bitcoin, John Oliver on Data Brokers, Russian Cyberattack against Ukrainian Power Grid Prevented, Industrial Control System Malware Discovered, Upcoming Speaking Engagements

March 15, 2022: Secret CIA Data Collection Program, Vendors are Fixing Security Flaws Faster, Possible Government Surveillance of the Otter.ai Transcription App, Stealing Bicycles by Swapping QR Codes, A New Cybersecurity "Social Contract", Bypassing Apple's AirTag Security, An Elaborate Employment Con in the Internet Age, Privacy Violating COVID Tests, Insurance Coverage for NotPetya Losses, Decrypting Hive Ransomware Data, Vulnerability in Stalkerware Apps, Details of an NSA Hacking Operation, Samsung Encryption Flaw, Hacking Alexa through Alexa's Speech, Using Radar to Read Body Language, Fraud on Zelle, Where's the Russia-Ukraine Cyberwar?, Leak of Russian Censorship Data, Upcoming Speaking Events

February 15, 2022: An Examination of the Bug Bounty Marketplace, UK Government to Launch PR Campaign Undermining End-to-End Encryption, Are Fake COVID Testing Sites Harvesting Data?, San Francisco Police Illegally Spying on Protesters, China's Olympics App Is Horribly Insecure, Linux-Targeted Malware Increased by 35%, Merck Wins Insurance Lawsuit re NotPetya Attack, New DeadBolt Ransomware Targets NAS Devices, Tracking Secret German Organizations with Apple AirTags, Twelve-Year-Old Linux Vulnerability Discovered and Patched, Me on App Store Monopolies and Security, Finding Vulnerabilities in Open Source Projects, Interview with the Head of the NSA's Research Directorate, The EARN IT Act Is Back, Amy Zegart on Spycraft in the Internet Age, Breaking 256-bit Elliptic Curve Encryption with a Quantum Computer, Bunnie Huang's Plausibly Deniable Database, On the Irish Health Services Executive Hack, Upcoming Speaking Engagements

January 15, 2022: More Log4j News, More on NSO Group and Cytox: Two Cyberweapons Arms Manufacturers, Stolen Bitcoins Returned, Apple AirTags Are Being Used to Track People and Cars, More Russian Cyber Operations against Ukraine, People Are Increasingly Choosing Private Web Search, Norton's Antivirus Product Now Includes an Ethereum Miner, Fake QR Codes on Parking Meters, Apple's Private Relay Is Being Blocked, Faking an iPhone Reboot, Using Foreign Nationals to Bypass US Surveillance Restrictions, Using EM Waves to Detect Malware, Upcoming Speaking Engagements

Earlier issues of Crypto-Gram are available here:
<https://www.schneier.com/crypto-gram/>

Significant Articles about Schneier

"*A Hacker's Mind* (book review)," *Booklist*, January 1, 2023.

"*Firewalls Don't Stop Dragons* 300th Episode" (podcast) November 28, 2022.

"Book Review: *A Hacker's Mind*," *Kirkus Reviews*, November 16, 2022.

"'Hacking' the Legal System," Bruce Schneier interview, *Aiming for the Moon* podcast, September 11, 2022.

"Bruce Schneier on the Crypto/Blockchain Disaster," *Cyber Protection Magazine*, August 11, 2022.

"Understanding Crypto 6: Bruce Schneier: Security, Trust, and Blockchain," *Rational Reminder*, July 8, 2022.

"Schneier: 'Le votazioni elettroniche? Non fatelo, non è sicuro'," *Cybersecurity 360*, July 04, 2022.

"Expert Interviews: Hacktivism," *Cyber.RAR*, June 29, 2022.

"Why AIs Will Become Hackers," *Dark Reading*, June 09, 2022.

"Schneier on Security for Tomorrow's Software," *The Changelog*, May 20, 2022.

"Unscripted with Bruce Schneier," *PSICC Data Privacy Week 2022*, February 04, 2022.

"Bruce Schneier on Regulating at the Pace of Tech," *Transform*, February 01, 2022.

"History of Hacking," *Cybercrime Magazine*, January 29, 2022.

"We Have to Trust Technology," *Conversation with Nobel Minds*, January 09, 2022.

"Bruce Schneier on Regulating at the Pace of Tech," *Transform*, December 30, 2021.

"*Click Here to Kill Everybody*," *Conversation with Nobel Minds*, December 26, 2021.

“Who’s Controlling the Internet?” *Project Save the World*, October 28, 2021.

“Bruce Schneier’s book *Secrets and Lies*,” *Byte*, October 18, 2021.

“”מירישעה אלא מירקאה מיעצבם אל רתויב תונכוסמה תוצירפה תא”,” *Calcalist*, September 08, 2021.

“Click Here To Kill Everybody,” *Power Corrupts*, September 07, 2021.

“Bruce Schneier: We Are Asking the Wrong Cybersecurity Questions,” *CDO Trends*, August 23, 2021.

“Secure Ventures Podcast,” *Secure Ventures with Kyle McNulty*, July 27, 2021.

“Going Meta: A Conversation and AMA with Bruce Schneier,” *8th Layer Insights*, July 20, 2021.

“The Coming AI Hackers. How Will They Put Society At Risk?,” *Cybercrime Magazine*, June 15, 2021.

“The Coming AI Hackers,” *Exponential View*, June 09, 2021.

“The Next Phase in Cyber Warfare,” *The Red Line*, May 16, 2021.

“When AI Becomes the Hacker,” *Dark Reading*, May 13, 2021.

“Hacking Is a Task AI Will Excel at (And We Are Not Far from That Point),” *ZDNet*, May 06, 2021.

“Bruce Schneier Wants You to Make Software Better,” *IEEE Spectrum*, April 28, 2021.

“Data, Surveillance & Internet Security with Bruce Schneier,” *CSINT Conversations*, March 03, 2021.

“Artificial Intelligence in Politics,” *Unpublished Cafe*, February 19, 2021.

“Cybersecurity: Same Threats, New Challenges,” *Forbes*, January 19, 2021.

“Bruce Schneier on Technology Security, Social Media, and Regulation,” *GrowthPolicy*, January 13, 2021.

“The Solarwinds Hack Is Stunning. Here’s What Should Be Done,” *CNN*, January 5, 2021.

“The US Has Suffered a Massive Cyberbreach. It’s Hard to Overstate How Bad It Is,” *Guardian*, December 24, 2020.

“The Peril of Persuasion in the Big Tech Age,” *Foreign Policy*, December 11, 2020.

“What Makes Trump’s Subversion Efforts So Alarming? His Collaborators,” *New York Times*, November 23, 2020.

“The Unrelenting Horizonlessness of the Covid World,” *CNN*, September 25, 2020.

“The Twitter Hacks Have to Stop,” *Atlantic*, July 18, 2020.

“Bruce Schneier says we need to embrace inefficiency to save our economy,” *Quartz*, June 30, 2020.

“The Public Good Requires Private Data,” *Foreign Policy*, May 16, 2020.

“Heise Webinar,” *Heise Events*, April 15, 2020.

“An Interview with Bruce Schneier, Renowned Security Technologist,” *The Politic*, April 1, 2020.

“Breaking Down the Huawei v. Pentagon Dispute,” *Federal Drive*, March 26, 2020.

“How to Detect Coronavirus Myths, Scams and Fake News: Security Guru Bruce Schneier Weighs In On COVID-19,” *Seattle 24x7*, March 15, 2020.

“#RSAC: How to Hack Society,” *Infosecurity*, February 27, 2020.

“What’s the Best Way to Use the Cloud to Store Personal Data?,” *The Wall Street Journal*, February 23, 2020.

“Bruce Schneier: On the Future of Public-Interest Tech,” *Humans of InfoSec*, February 19, 2020.

“Not Just about the Data,” *Science Node*, February 17, 2020.

“Bruce Schneier on How Insecure Electronic Voting Could Break the United States—and Surveillance Without Tyranny,” *80000 Hours*, October 25, 2019.

“‘Click Here To Kill Everybody’ Book Review by Cybersecurity Expert Scott Schober,” *YouTube*, October 18, 2019.

“What You Need to Know about Security in Government,” *Code for America*, August 29, 2019.

“Wanted: ‘Public-Interest Technologists’ to Inform Raging Debates on Cybersecurity Policy,” *Inside Cybersecurity*, August 12, 2019.

“Autonomous Vehicle Security Deep Dive w/Bruce Schneier,” *Thinking through Autonomy*, August 7, 2019.

“Bruce Schneier Talks the Cybersecurity Risks of an Autonomous Future,” *Thinking Through Autonomy*, July 22, 2019.

“‘Tu Coche Ya Está Conectado a Internet y Ahora Cualquiera Puede Usarlo para Matarte,’” *El Confidencial*, July 11, 2019.

“Bruce Schneier Is Leaving IBM,” *SecureWorld*, July 3, 2019.

“Bruce Schneier Moves on from IBM,” *SecurityWeek*, July 2, 2019.

“Don’t Tell Alice and Bob: Security Maven Bruce Schneier Is Leaving IBM,” *The Register*, July 1, 2019.

“SwigCast, Episode 2: Encryption,” *The Daily Swig*, June 27, 2019.

“Apocalipsis digital: cómo evitar que el ser humano se extinga por culpa de internet,” *El Mundo*, June 25, 2019.

“How Government Can Secure Us in the Internet+ Era,” *The Government We Need*, June 18, 2019.

“Bruce Schneier on Cybersecurity,” *Challenging Opinions*, June 3, 2019.

“Scrambled Hidden Potato Device with Bruce Schneier,” *Random but Memorable*, May 21, 2019.

“Black Hat Q&A: Bruce Schneier Calls For Public-Interest Technologists,” *Dark Reading*, May 20, 2019.

“Summit 2019: Cybersecurity and Public Interest Tech with Bruce Schneier,” *Code for America*, April 24, 2019.

“Is Online Convenience Worth the Trade-Off for Less Cybersecurity?,” *BYU Radio*, April 15, 2019.

“傳奇密碼學大師專訪：別輕信物聯網,” *Business Weekly*, April 10, 2019.

“Collective Intelligence Podcast, Bruce Schneier on Public-Interest Tech,” *Flashpoint*, April 1, 2019.

“Q&A: Crypto-Guru Bruce Schneier on Teaching Tech to Lawmakers, Plus Privacy Failures—and a Call to Techies to Act,” *The Register*, March 15, 2019.

“Security Concerns Rise As More Household Items Join The Internet World,” *Wisconsin Public Radio*, January 29, 2019.

“The Existential Threat of Hyper-Connecting the World,” *Decentralize This!*, January 29, 2019.

“Data Privacy Day Episode of ‘Firewalls Don’t Stop Dragons,’” *Firewalls Don’t Stop Dragons*, January 28, 2019.

“The Missing Piece in Cybersecurity is Government,” *Defence24*, January 25, 2019.

“The Security Book Everyone in Government Must Read in 2019,” *GovFresh*, December 23, 2018.

“Ben’s Book of the Month: Review of ‘Click Here to Kill Everybody: Security and Survival in a Hyper-connected World,’” *RSA Conference Blog*, November 30, 2018.

“Has Your Toaster Got Cyber-Security? It May Soon Need It,” *Catholic Herald*, November 29, 2018.

“Click Here to Kill Everybody, IoT Security and Cryptography,” *The NULLCON Podcast*, November 26, 2018.

“Click Here to Kill Everybody: Security, Privacy, Social Media and Politics,” *Fringe.fm*, November 12, 2018.

“Harry Shearer Interviews Bruce Schneier,” *Le Show*, November 11, 2018.

“Click Here to Kill Everybody,” *The Cyberwire*, November 9, 2018.

“Click Here To Kill Everybody,’ with Bruce Schneier,” *Steal This Show*, November 1, 2018.

“A Future Where Everything Becomes a Computer Is as Creepy as You Feared,” *The New York Times*, October 10, 2018.

“How to Keep the Internet of Things From Killing Us All,” *Pacific Standard*, October 9, 2018.

“The Biggest Cybersecurity Threat You Never Thought That Much About Is the Factory,” *Marketplace*, October 9, 2018.

“Bruce Schneier’s Click Here to Kill Everybody Reveals the Looming Cybersecurity Crisis,” *CSO*, October 3, 2018.

“Cybersecurity, the Internet of Things, and Social Media,” *Social Media and Politics Podcast*, September 30, 2018.

“‘Click Here to Kill Everybody’: A Berkman Klein Center Book Talk,” *Berkman Klein Center*, September 25, 2018.

“Publisher’s Weekly Review of *Click Here to Kill Everybody*,” *Publisher’s Weekly*, September 24, 2018.

“Cyberattacks and Survival in a Hyperconnected World,” *Hidden Forces Podcast*, September 18, 2018.

“The Lawfare Podcast: Bruce Schneier on ‘Click Here to Kill Everybody,’” *The Lawfare Podcast*, September 18, 2018.

“Bruce Schneier Book Talk with Ben Wizner,” *Center on National Security at Fordham Law*, September 17, 2018.

“Open Letters Review on *Click Here to Kill Everybody*,” *Open Letters Review*, September 14, 2018.

“Internet Plus: Now Everything Can Be Hacked!,” *CBC Radio*, September 14, 2018.

“The Cyberlaw Podcast: Click Here to Kill Everybody,” *The Cyberlaw Podcast*, September 11, 2018.

“Takeaways from Bruce Schneier’s New Book,” *Politico*, September 11, 2018.

“Podcast Episode 111: Click Here to Kill Everybody and CyberSN on Why Security Talent Walks,” *The Security Ledger*, September 10, 2018.

“Book Launch at The Aspen Institute,” *The Aspen Institute*, September 10, 2018.

“For Safety’s Sake, We Must Slow Innovation in Internet-Connected Things,” *MIT Technology Review*, September 6, 2018.

“Book Review: Click Here to Kill Everybody,” *Virus Bulletin*, September 6, 2018.

“Vulnerabilities of an Inter-connected World,” *Midday on WNYC*, September 5, 2018.

“Book Review: ‘Click Here To Kill Everybody,’” *Harris Online*, September 4, 2018.

“Schneier’s ‘Click Here To Kill Everybody,’” *Boing Boing*, September 4, 2018.

“Hackers Used a Fish Tank to Break into a Vegas Casino. We’re All in Trouble,” *The Washington Post*, September 4, 2018.

“Kirkus Review: Click Here To Kill Everybody,” *Kirkus Reviews*, September 4, 2018.

“Radio Interview on ‘Click Here To Kill Everybody,’” *NPR 1A*, September 4, 2018.

“How to Survive in a Hyperconnected World,” *Ford Foundation*, August 29, 2018.

“Governments Want Your Smart Devices to Have Stupid Security Flaws,” *Nature*, August 28, 2018.

“Click Here to Kill Everybody by Bruce Schneier,” *Financial Times*, August 26, 2018.

“Newsmaker Interview: Bruce Schneier on ‘Going Dark’ and the Crypto Arms Race,” *Threatpost*, July 16, 2018.

“[Book Review] Data and Goliath by Bruce Schneier,” *Center for Digital Society*, May 9, 2018.

“Schneier Talks Cyber Regulations, Slams U.S. Lawmakers,” *SearchSecurity*, April 19, 2018.

“Collective Intelligence Podcast, Bruce Schneier on Data Collection and Privacy,” *Flashpoint*, April 17, 2018.

“The Truth About Terrorism with Bruce Schneier,” *Kensington TV*, January 11, 2018.

“Schneier: It’s Time to Regulate IoT to Improve Cyber-Security,” *eWeek*, November 15, 2017.

“An Interview with Bruce Schneier on the Internet of Things, Global Surveillance, and Cybersecurity,” *ExpressVPN*, October 24, 2017.

“The Cybersecurity Canon: Data and Goliath,” *Palo Alto Networks*, October 8, 2017.

“On Internet Privacy, Be Very Afraid,” *Harvard Gazette*, August 24, 2017.

“Is It Time To Regulate the IoT?,” *SecTor*, August 11, 2017.

“Surveillance Is the Business Model of the Internet,” *OpenDemocracy*, July 18, 2017.

Earlier news articles are available here: <https://www.schneier.com/news/>

Previous Declarations and Depositions

Chasom Brown, William Byatt, Jeremy David, Christopher Castillo, and Monique Trujillo, individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-03664-YGR-SVK, United States District Court for the Northern California District. Expert witness for Brown et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2022).

Mon Cheri Bridals, LLC and Maggie Sottero Designs, LLC v. Cloudflare, Inc., Case No. 2:18-cv-09453-MWF-AS, United States District Court for the Central District of California. Expert witness for Cloudflare, Inc., Fenwick & West, LLP, attorneys. Declarations (2020 and 2021).

Fortinet, Inc. v. BT Americas, Inc., Case No. IPR2019-01324, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent No. 7,895,641. Expert witness for BT Americas, Inc., Proskaur Rose LLP, attorneys. Declaration (2019).

United to Protect Democracy et al. v. Presidential Advisory Commission on Election Integrity et al., Civil Action No. 1:17-cv-02016, United States District Court for the District of Columbia. Declaration (2017).

Koninklijke Philips N.V. and U.S. Philips Corp. v. HTC Corp. and HT America, Civil Action No. 15-1126-GMS, United States District Court for the District of Delaware, concerning U.S. Patent Nos. 8.543.819 and 9.436.809. Expert witness for HTC Corp., Perkins Coie LLP, attorneys. Declaration (2017).

Ex parte reexamination of U.S. Patent No. 6,760,752. Expert witness for the patent holder Zix Corp., Haynes and Boone, LLC attorneys. Declaration (2017).

Great West Casualty Co., BITCO General Insurance Corp., and BITCO National Insurance Co. v. Transpacific IP Ltd, Case No. IPR2015-00x, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent No. 8,929,555. Expert witness for Great West Casualty Co., BITCO General Insurance Corp., and BITCO National Insurance Co., Sidley Austin LLP attorneys. Declaration (2015).

Unikey Technologies, Inc. v. Assa Abloy AB, Cases No. IPR2015-01440 and IPR2015-01441, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 7,706,778 and 8,150,374. Expert witness for UniKey Technologies, Inc., Proskauer Rose LLP attorneys. Declaration (2015).

Epicor Software Corp. v. Protegrity Corp., Case Nos. CBM2015-00002 and CBM2015-00006, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 6,321,201 and 8,402,281. Expert witness for Epicor Software Corp., Cantor Colborn LLP attorneys. Declaration (2015) and deposition (2015).

Quantum World Corp. v. Dell, Inc. Civil Action No. A-11-CA-688-SS, United States District Court for the Western Division of Texas regarding U.S. Patent Nos. 6,763,364, 7,096,242, and 7,752,247. Expert witness for Dell, Inc., Alston & Bird attorneys. Declaration and deposition (2015).

Entrust, Inc. v. Secure Axxess, LLC, Case No. CBM2015-0027, Covered Business Method Review United States Patent and Trademark Office before the Patent Trial and Appeal Board concerning Patent No. 7,631,191. Expert witness for Entrust, Inc., Crowell & Morning LLP attorneys. Declaration (2014) and deposition (2015).

Apple, Inc. v. Achates Reference Publishing, Inc., Case Nos. IPR 13-00080 and IPR 13-00081, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 6,173,403 and 5,982,889. Expert witness for Apple, Inc., DiNovo Price LLP and Sidley Austin LLP attorneys. Declaration and deposition.

Research in Motion Corp. v. Innovative Sonic, Docket No. 377211US, Inter Partes Review, United States Patent and Trademark Office regarding Patent No. 6,925,183. Expert witness for Research In Motion Corp., Expert witness for Research in Motion Corp., Oblon Spivak attorneys. Declaration.

Walker Digital, LLC v. MySpace, Inc., et al., Civil Action No. 1:11-cv-00318-LPS, United States District Court for the District of Delaware, concerning U.S. Patent Nos. 5,884,270 and 5,884,272. Deposition as patent author.

Walker Digital, LLC v. Google, Inc., et al., Civil Action No. 11-309-SLR, United States District Court for the District of Delaware, concerning U.S. Patent No. 5,768,382. Deposition as patent author.

Bruce Schneier CV: Previous Declarations and Depositions**58**

TecSec, Inc. v. International Business Machines Corp., et al., Civil Action No. 1:10-cv-00115-LMB/TCB, United States District Court for the Eastern District of Virginia (Alexandria) concerning U.S. Patents No. 5,369,702 and 6,549,623. Expert witness for TecSec, Inc., Hunton & Williams LLP, attorneys for TecSec, Inc. Declaration and deposition.

Luciano F. Paone v. Microsoft Corp., Civil Action No. CV-07-2973 (E.D. NY), United States District Court for the Northern District of California concerning U.S. Patent No. 6,259,789. Expert witness for Microsoft Corp., Kirkland & Ellis attorneys. Declaration and deposition.

Fred and Kathleen Stark v. The Seattle Seahawks LLC, Civil Action No. CV-06-1719 JLR, United States District Court for the Western District of Washington at Seattle concerning the efficacy of pat-down searches. Expert witness for Stark, Danielson Harrigan Leyh & Tollefson LLC, attorneys for Stark. Declaration and deposition.

Gordon Johnston v. The Tampa Sports Authority et al., Civil Action No. 8-05-cv-02191-JDW-MAP, United States District Court for the Middle District of Florida Tampa Division. concerning the efficacy of pat-down searches. Expert witness for Johnston. Declaration.

EXPERT REPORT OF BRUCE SCHNEIER

20 February 2023

Appendix 3
Readability Tests
of
Google Terms of Service
Google Privacy Policy

tested with
Readability Calculator

https://www.online-utility.org/english/readability_test_and_improve.jsp

Google Terms of Service

- 4 versions from April 14, 2014 to January 25, 2022.
- Total number of words: 11,335
- Flesch Reading Ease range: 42.54 to 31.21

Google Terms of Service (April 14, 2014)

Number of characters (without spaces):	9,347.00
Number of words:	1,920.00
Number of sentences:	99.00
Lexical Density:	49.90
Average number of characters per word:	4.87
Average number of syllables per word:	1.71
Average number of words per sentence:	19.39
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	12.24
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	11.33
Flesch Kincaid Grade level:	12.14
ARI (Automated Readability Index):	11.20
SMOG:	13.56
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	42.54

Google Terms of Service (October 25, 2017)

Number of characters (without spaces):	9,349.00
Number of words:	1,920.00
Number of sentences:	98.00
Lexical Density:	49.90
Average number of characters per word:	4.87
Average number of syllables per word:	1.71
Average number of words per sentence:	19.59
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	12.34
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	11.35
Flesch Kincaid Grade level:	12.23
ARI (Automated Readability Index):	11.30
SMOG:	13.63
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	42.29

Google Terms of Service (March 31, 2020)

Number of characters (without spaces):	19,718.00
Number of words:	3,978.00
Number of sentences:	130.00
Lexical Density:	53.62
Average number of characters per word:	4.96
Average number of syllables per word:	1.71
Average number of words per sentence:	30.60
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	17.14
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.41
Flesch Kincaid Grade level:	16.49
ARI (Automated Readability Index):	17.22
SMOG:	16.04
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	31.35

Google Terms of Service (January 25, 2022)

Number of characters (without spaces):	17,323.00
Number of words:	3,517.00
Number of sentences:	111.00
Lexical Density:	52.97
Average number of characters per word:	4.93
Average number of syllables per word:	1.70
Average number of words per sentence:	31.68
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	17.25
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.26
Flesch Kincaid Grade level:	16.78
ARI (Automated Readability Index):	17.61
SMOG:	16.05
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	31.21

Google Privacy Policy

- 19 versions from June 28, 2016 to December 15, 2022.
- Total number of words: 127,488
- Flesch Reading Ease range: 28.60 to 36.79

Google Privacy Policy (June 28, 2016)

Number of characters (without spaces):	20,613.00
Number of words:	4,064.00
Number of sentences:	194.00
Lexical Density:	53.47
Average number of characters per word:	5.07
Average number of syllables per word:	1.76
Average number of words per sentence:	20.95
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	14.02
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.64
Flesch Kincaid Grade level:	13.33
ARI (Automated Readability Index):	12.93
SMOG:	13.89
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	36.79

Google Privacy Policy (August 29, 2016)

Number of characters (without spaces):	20,673.00
Number of words:	4,075.00
Number of sentences:	194.00
Lexical Density:	53.52
Average number of characters per word:	5.07
Average number of syllables per word:	1.76
Average number of words per sentence:	21.01
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	14.05
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.65
Flesch Kincaid Grade level:	13.36
ARI (Automated Readability Index):	12.97
SMOG:	13.91
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	36.66

Google Privacy Policy (March 1, 2017)

Number of characters (without spaces):	20,663.00
Number of words:	4,075.00
Number of sentences:	194.00
Lexical Density:	53.52
Average number of characters per word:	5.07
Average number of syllables per word:	1.76
Average number of words per sentence:	21.01
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	14.05
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.64
Flesch Kincaid Grade level:	13.36
ARI (Automated Readability Index):	12.96
SMOG:	13.91
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	36.68

Google Privacy Policy (April 17, 2017)

Number of characters (without spaces):	20,675.00
Number of words:	4,078.00
Number of sentences:	194.00
Lexical Density:	53.51
Average number of characters per word:	5.07
Average number of syllables per word:	1.76
Average number of words per sentence:	21.02
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	14.05
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.63
Flesch Kincaid Grade level:	13.36
ARI (Automated Readability Index):	12.96
SMOG:	13.91
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	36.69

Google Privacy Policy (October 2, 2017)

Number of characters (without spaces):	20,722.00
Number of words:	4,086.00
Number of sentences:	193.00
Lexical Density:	53.57
Average number of characters per word:	5.07
Average number of syllables per word:	1.76
Average number of words per sentence:	21.17
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	14.13
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.65
Flesch Kincaid Grade level:	13.43
ARI (Automated Readability Index):	13.04
SMOG:	13.97
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	36.50

Google Privacy Policy (December 18, 2017)

Number of characters (without spaces):	13,998.00
Number of words:	2,707.00
Number of sentences:	116.00
Lexical Density:	53.97
Average number of characters per word:	5.17
Average number of syllables per word:	1.82
Average number of words per sentence:	23.34
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.69
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	13.37
Flesch Kincaid Grade level:	14.94
ARI (Automated Readability Index):	14.59
SMOG:	15.19
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	29.54

Google Privacy Policy (May 25, 2018)

Number of characters (without spaces):	36,114.00
Number of words:	7,233.00
Number of sentences:	297.00
Lexical Density:	54.62
Average number of characters per word:	4.99
Average number of syllables per word:	1.75
Average number of words per sentence:	24.35
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.02
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.38
Flesch Kincaid Grade level:	14.55
ARI (Automated Readability Index):	14.26
SMOG:	14.49
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	34.12

Google Privacy Policy (January 22, 2019)

Number of characters (without spaces):	36,330.00
Number of words:	7,276.00
Number of sentences:	298.00
Lexical Density:	54.60
Average number of characters per word:	4.99
Average number of syllables per word:	1.75
Average number of words per sentence:	24.42
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.07
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.38
Flesch Kincaid Grade level:	14.57
ARI (Automated Readability Index):	14.30
SMOG:	14.52
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	34.07

Google Privacy Policy (October 15, 2019)

Number of characters (without spaces):	37,106.00
Number of words:	7,441.00
Number of sentences:	303.00
Lexical Density:	54.47
Average number of characters per word:	4.99
Average number of syllables per word:	1.75
Average number of words per sentence:	24.56
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.12
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.35
Flesch Kincaid Grade level:	14.64
ARI (Automated Readability Index):	14.34
SMOG:	14.55
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	33.87

Google Privacy Policy (December 19, 2019)

Number of characters (without spaces):	39,638.00
Number of words:	7,892.00
Number of sentences:	330.00
Lexical Density:	54.60
Average number of characters per word:	5.02
Average number of syllables per word:	1.76
Average number of words per sentence:	23.92
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.02
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.53
Flesch Kincaid Grade level:	14.52
ARI (Automated Readability Index):	14.18
SMOG:	14.57
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	33.52

Google Privacy Policy (March 31, 2020)

Number of characters (without spaces):	39,932.00
Number of words:	7,954.00
Number of sentences:	337.00
Lexical Density:	54.63
Average number of characters per word:	5.02
Average number of syllables per word:	1.76
Average number of words per sentence:	23.60
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	14.86
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.50
Flesch Kincaid Grade level:	14.39
ARI (Automated Readability Index):	14.02
SMOG:	14.47
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	33.93

Google Privacy Policy (July 1, 2020)

Number of characters (without spaces):	42,703.00
Number of words:	8,479.00
Number of sentences:	357.00
Lexical Density:	54.72
Average number of characters per word:	5.04
Average number of syllables per word:	1.77
Average number of words per sentence:	23.75
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.03
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.60
Flesch Kincaid Grade level:	14.52
ARI (Automated Readability Index):	14.17
SMOG:	14.56
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	33.27

Google Privacy Policy (August 28, 2020)

Number of characters (without spaces):	42,775.00
Number of words:	8,491.00
Number of sentences:	358.00
Lexical Density:	54.74
Average number of characters per word:	5.04
Average number of syllables per word:	1.77
Average number of words per sentence:	23.72
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.02
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.61
Flesch Kincaid Grade level:	14.51
ARI (Automated Readability Index):	14.16
SMOG:	14.55
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	33.29

Google Privacy Policy (September 30, 2020)

Number of characters (without spaces):	42,602.00
Number of words:	8,449.00
Number of sentences:	353.00
Lexical Density:	54.72
Average number of characters per word:	5.04
Average number of syllables per word:	1.77
Average number of words per sentence:	23.93
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.12
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.65
Flesch Kincaid Grade level:	14.61
ARI (Automated Readability Index):	14.29
SMOG:	14.62
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	32.96

Google Privacy Policy (February 4, 2021)

Number of characters (without spaces):	42,966.00
Number of words:	8,518.00
Number of sentences:	354.00
Lexical Density:	54.78
Average number of characters per word:	5.04
Average number of syllables per word:	1.77
Average number of words per sentence:	24.06
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.14
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.66
Flesch Kincaid Grade level:	14.65
ARI (Automated Readability Index):	14.36
SMOG:	14.66
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	32.86

Google Privacy Policy (July 1, 2021)

Number of characters (without spaces):	43,261.00
Number of words:	8,582.00
Number of sentences:	357.00
Lexical Density:	54.77
Average number of characters per word:	5.04
Average number of syllables per word:	1.77
Average number of words per sentence:	24.04
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.12
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.64
Flesch Kincaid Grade level:	14.64
ARI (Automated Readability Index):	14.33
SMOG:	14.65
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	32.94

Google Privacy Policy (February 10, 2022)

Number of characters (without spaces):	45,246.00
Number of words:	8,991.00
Number of sentences:	366.00
Lexical Density:	54.82
Average number of characters per word:	5.03
Average number of syllables per word:	1.76
Average number of words per sentence:	24.57
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.31
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.62
Flesch Kincaid Grade level:	14.80
ARI (Automated Readability Index):	14.56
SMOG:	14.74
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	32.70

Google Privacy Policy (October 4, 2022)

Number of characters (without spaces):	46,027.00
Number of words:	9,141.00
Number of sentences:	371.00
Lexical Density:	54.82
Average number of characters per word:	5.04
Average number of syllables per word:	1.76
Average number of words per sentence:	24.64
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	15.32
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	12.64
Flesch Kincaid Grade level:	14.83
ARI (Automated Readability Index):	14.61
SMOG:	14.74
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	32.61

Google Privacy Policy (December 15, 2022)

Number of characters (without spaces):	30,321.00
Number of words:	5,956.00
Number of sentences:	227.00
Lexical Density:	55.31
Average number of characters per word:	5.09
Average number of syllables per word:	1.79
Average number of words per sentence:	26.24
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index:	16.24
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index:	13.04
Flesch Kincaid Grade level:	15.79
ARI (Automated Readability Index):	15.67
SMOG:	15.46
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease:	28.60

Method

The texts of the current and archived versions of the following documents were copied and entered into the Readability Calculator at https://www.online-utility.org/english/readability_test_and_improve.jsp:

- Google Terms of Service: <https://policies.google.com/terms?hl=en-US>
- Google Privacy Policy: <https://policies.google.com/privacy?hl=en-US>

The Readability Calculator applies a variety of mathematical formulae to analyze the readability and comprehensibility of a text. The measures cited here are commonly used formulas for determining the readability of texts in English.

Readability Formulas

Gunning-Fog Index

https://en.wikipedia.org/wiki/Gunning_fog_index

In linguistics, the Gunning fog index is a readability test for English writing. The index estimates the years of formal education a person needs to understand the text on the first reading. For instance, a fog index of 12 requires the reading level of a United States high school senior (around 18 years old). The test was developed in 1952 by Robert Gunning, an American businessman who had been involved in newspaper and textbook publishing.

The Gunning fog index is calculated with the following algorithm:

- Select a passage (such as one or more full paragraphs) of around 100 words. Do not omit any sentences;
- Determine the average sentence length. (Divide the number of words by the number of sentences.);
- Count the “complex” words consisting of three or more syllables. Do not include proper nouns, familiar jargon, or compound words. Do not include common suffixes (such as -es, -ed, or -ing) as a syllable;
- Add the average sentence length and the percentage of complex words; and
- Multiply the result by 0.4.

The complete formula is

$$0.4 \left[\left(\frac{\text{words}}{\text{sentences}} \right) + 100 \left(\frac{\text{complex words}}{\text{words}} \right) \right]$$

Coleman Liau index

https://en.wikipedia.org/wiki/Coleman%E2%80%93Liau_index

The Coleman–Liau index is a readability test designed by Meri Coleman and T. L. Liau to gauge the understandability of a text. Like the Flesch–Kincaid Grade Level, Gunning fog index, SMOG index, and Automated Readability Index, its output approximates the U.S. grade level thought necessary to comprehend the text.

Like the ARI but unlike most of the other indices, Coleman–Liau relies on characters instead of syllables per word. Although opinion varies on its accuracy as compared to the syllable/word and complex word indices, characters are more readily and accurately counted by computer programs than are syllables.

The Coleman–Liau index is calculated with the following formula:

$$CLI = 0.0588L - 0.296S - 15.8$$

L is the average number of letters per 100 words and S is the average number of sentences per 100 words.

Flesch Kincaid Grade level

https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests

These readability tests are used extensively in the field of education. The “Flesch–Kincaid Grade Level Formula” instead presents a score as a U.S. grade level, making it easier for teachers, parents, librarians, and others to judge the readability level of various books and texts. It can also mean the number of years of education generally required to understand this text, relevant when the formula results in a number greater than 10. The grade level is calculated with the following formula:

$$0.39 \left(\frac{\text{total words}}{\text{total sentences}} \right) + 11.8 \left(\frac{\text{total syllables}}{\text{total words}} \right) - 15.59$$

The result is a number that corresponds with a U.S. grade level.

ARI (Automated Readability Index)

https://en.wikipedia.org/wiki/Automated_readability_index

The automated readability index (ARI) is a readability test for English texts, designed to gauge the understandability of a text. Like the Flesch–Kincaid grade level, Gunning fog index, SMOG index, Fry readability formula, and Coleman–Liau index, it produces an approximate representation of the US grade level needed to comprehend the text.

The formula for calculating the automated readability index is given below:

$$4.71 \left(\frac{\text{characters}}{\text{words}} \right) + 0.5 \left(\frac{\text{words}}{\text{sentences}} \right) - 21.43$$

where *characters* is the number of letters and numbers, *words* is the number of spaces, and *sentences* is the number of sentences, which were counted manually by the typist when the above formula was developed. Non-integer scores are always rounded up to the nearest whole number, so a score of 10.1 or 10.6 would be converted to 11.

Unlike the other indices, the ARI, along with the Coleman–Liau, relies on a factor of characters per word, instead of the usual syllables per word. Although opinion varies on its accuracy as compared to the syllables/word and complex words indices, characters/word is often faster to calculate, as the number of characters is more readily and accurately counted by computer programs than syllables. In fact, this index was designed for real-time monitoring of readability on electric typewriters.

SMOG (Simple Measure of Gobbledygook)

<https://en.wikipedia.org/wiki/SMOG>

The SMOG grade is a measure of readability that estimates the years of education needed to understand a piece of writing. SMOG is an acronym for “Simple Measure of Gobbledygook”.

The formula for calculating the SMOG grade was developed by G. Harry McLaughlin as a more accurate and more easily calculated substitute for the Gunning fog index and published in 1969. To make

calculating a text's readability as simple as possible an approximate formula was also given — count the words of three or more syllables in three 10-sentence samples, estimate the count's square root (from the nearest perfect square), and add 3.

To calculate SMOG Index

- Count a number of sentences (at least 30)
- In those sentences, count the polysyllables (words of 3 or more syllables).
- Calculate using

$$\text{grade} = 1.0430 \sqrt{\text{number of polysyllables} \times \frac{30}{\text{number of sentences}}} + 3.1291$$

Flesch Reading Ease

https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests

In the Flesch reading-ease test, higher scores indicate material that is easier to read; lower numbers mark passages that are more difficult to read. The formula for the Flesch reading-ease score (FRES) test is:

$$206.835 - 1.015 \left(\frac{\text{total words}}{\text{total sentences}} \right) - 84.6 \left(\frac{\text{total syllables}}{\text{total words}} \right)$$

Scores can be interpreted as shown in the table below.

Score	School level (US)	Notes
100.00–90.00	5th grade	Very easy to read. Easily understood by an average 11-year-old student.
90.0–80.0	6th grade	Easy to read. Conversational English for consumers.
80.0–70.0	7th grade	Fairly easy to read.
70.0–60.0	8th & 9th grade	Plain English. Easily understood by 13- to 15-year-old students.
60.0–50.0	10th to 12th grade	Fairly difficult to read.
50.0–30.0	College	Difficult to read.
30.0–10.0	College graduate	Very difficult to read. Best understood by university graduates.
10.0–0.0	Professional	Extremely difficult to read. Best understood by university graduates.

Lexical Density

https://en.wikipedia.org/wiki/Lexical_density

Lexical density is a concept in computational linguistics that measures the structure and complexity of human communication in a language.[1] Lexical density estimates the linguistic complexity in a written or spoken composition from the functional words (grammatical units) and content words (lexical units,

lexemes). One method to calculate the lexical density is to compute the ratio of lexical items to the total number of words. Another method is to compute the ratio of lexical items to the number of higher structural items in a composition, such as the total number of clauses in the sentences.

Ure proposed the following formula in 1971 to compute the lexical density of a sentence

$$L_d = \frac{\text{The number of lexical items}}{\text{The total number of words}} * 100$$

Expert Report of Bruce Schneier

February 20, 2023

Appendix 1

Documents Considered

Addendum (June 21 2023)

As explained in Professor Schneier's objections and responses to Google's Notice of Subpoena, Mr. Schneier discovered that some public documents he considered in the course of forming his opinions in his report were inadvertently omitted from Appendix 1. These additional materials are:

Iman M. Almomani and Aala Al Khayer, "A comprehensive analysis of the Android permissions system," *IEEE Access* 8, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9272963> (November 30, 2020).

Australian Competition and Consumer Commission v Google LLC (No 4) [2022] FCA 942 (Thawley J), <http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2022/942.html> (August 12, 2022).

Parnika Bhat and Kamlesh Dutta, "A survey on various threats and current state of security in Android platform," *ACM Computing Surveys* 52, no. 1, <http://acm.mementodepot.org/pubs/journals/csur/3309872/3301285/3301285.pdf> (February 2019).

Reuben Binns, et al., "Third party tracking in the mobile ecosystem," WebSci'18: 10th ACM Conference on Web Science, May 27-30, 2018, Amsterdam, Netherlands, <https://arxiv.org/pdf/1804.03603.pdf> (May 2018).

Jorge Blasco, et al., "Detection of app collusion potential using logic programming," *Journal of Network and Computer Applications* 105, <https://arxiv.org/abs/1706.02387> (2018).

Kristen E. Busch, "What hides in the shadows: Deceptive design of dark patterns," *In Focus*, Congressional Research Service, <https://sgp.fas.org/crs/misc/IF12246.pdf> (November 4, 2022).

L. Ceci, "App tracking and mobile privacy: Statistics and facts," *Statista*, <https://www.statista.com/topics/9460/app-tracking-and-mobile-privacy> (May 23, 2022).

Shruthi Chivukula, et al., "Nothing comes before profit": Asshole design in the wild," *CHI EA '19: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, Paper No.: LBW1314, <https://dl.acm.org/doi/10.1145/3290607.3312863> (May 2019).

John F. Clark, "History of mobile applications (Slide deck)," University of Kentucky, <https://www.uky.edu/~jclark/mas490apps/History%20of%20Mobile%20Apps.pdf> (no date).

Michael Cobb, "How do SDKs for ad networks cause data leaks?" *Tech Target*, <https://www.techtarget.com/searchsecurity/answer/How-do-SDKs-for-ad-networks-cause-data-leaks> (August 2018).

Jason Cohen, "These apps collect the most personal data," *PC Magazine*, <https://www.pcmag.com/news/sick-of-data-collection-try-these-apps-instead> (January 11, 2022).

Devin Coldewey, "Study calls out 'dark patterns' in Facebook and Google that push users toward less privacy," *TechCrunch*, <https://techcrunch.com/2018/06/27/study-calls-out-dark-patterns-in-facebook-and-google-that-push-users-towards-less-privacy> (June 27, 2018).

Ivan Dimitrov, "Invasive apps," *pCloud Blog*, <https://www.pcloud.com/invasive-apps> (March 5, 2021).

Vittoria Elliott, "Fertility and period apps can be weaponized in a post-Roe world," *WIRED*, <https://www.wired.com/story/fertility-data-weaponized> (June 7, 2022).

Sead Fadilpasic, "Shock horror - many top mobile apps secretly collect your data," *TechRadar*, <https://www.techradar.com/news/shock-horror-many-top-mobile-apps-secretly-collect-your-data> (October 7, 2022).

Eric Feltman, "Google Analytics 4 & Firebase: The evolution of mobile app measurement," Merkle Cardinal Path, <https://www.cardinalpath.com/blog/google-analytics-4-firebase-the-evolution-of-mobile-app-measurement> (January 22, 2021).

Tony Foley, "Google fined in Australia for data collection practices," *Cybersecurity Policy Report*, <https://www.vitalaw.com/news/cybersecurity-policy-report-google-fined-in-australia-for-data-collection-practices-aug-12-2022/cspd01390c39b73a774787b221bf1f86c37d8b> (August 12, 2022).

Stylianios Gisdakis, Thanassis Giannetsos and Panos Papadimitratos, "Android privacy C(R)ache: Reading your external storage and sensors for fun and profit," Second MobiHoc International Workshop on Privacy-Aware Mobile Computing (PAMCO 2016), Paderborn, Germany, <https://www.diva-portal.org/smash/get/diva2:878650/FULLTEXT01.pdf> (July 5, 2016).

Colin M. Gray, Shruthi Chivukula and Ahreum Lee, "What kind of work do "asshole designers" create? Describing properties of ethical concern on Reddit," *DIS '20: Proceedings of the 2020 ACM Designing Interactive Systems Conference*, <https://dl.acm.org/doi/abs/10.1145/3357236.3395486> (July 2020).

Colin M. Gray, et al., "End user accounts of dark patterns as felt manipulation," *Proceedings of the ACM Conference on Human-Computer Interaction 2021*, article 372, <https://dl.acm.org/doi/abs/10.1145/3479516> (2021).

Colin M. Gray, et al., "Dark patterns and the legal requirements of consent banners: An interaction criticism perspective," *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, <https://dl.acm.org/doi/10.1145/3411764.3445779> (May 2021).

Madeline Halpert, "Intuit to pay \$141 million to settle claims it deceived low-income users of TurboTax," *Forbes*, <https://www.forbes.com/sites/madelinehalpert/2022/05/04/intuit-to-pay-141-million-to-settle-claims-it-deceived-low-income-users-of-turbotax/?sh=6432658c39e4> (May 4, 2022).

N. Helberger, et al., "Choice architectures in the digital economy: Towards a new understanding of digital vulnerability," *Journal of Consumer Policy* 45, no. 2, <https://link.springer.com/article/10.1007/s10603-021-09500-5> (2022).

Tom Huddleston, Jr., "TikTok shares your data more than any other social media app — and it's unclear where it goes, study says," *Make It*, <https://www.cnn.com/2022/02/08/tiktok-shares-your-data-more-than-any-other-social-media-app-study.html> (February 8, 2022).

Cordilia James and Shara Tibken, "Period-tracker apps aim for anonymity following *Roe v. Wade* decision," *Wall Street Journal*, <https://www.wsj.com/articles/period-tracker-apps-aim-for-anonymity-following-roe-v-wade-decision-11656202089> (June 26, 2022).

Arjun Kharpal, "Facebook parent Meta agrees to pay \$725 million to settle Cambridge Analytica suit," NBC News, <https://www.nbcnews.com/tech/tech-news/facebook-parent-meta-agrees-pay-725-million-settle-cambridge-analytica-rcna63081> (December 23, 2022).

Brian Klais, "New research across 200 iOS apps hints that surveillance marketing is still going strong," *URL Genius*, <https://app.urlgeni.us/blog/new-research-across-200-ios-apps-hints-surveillance-marketing-may-still-be-going-strong> (January 20, 2022).

Martynas Klimas, "The data flows: How private are popular period tracker apps?" Surfshark, <https://surfshark.com/blog/period-track-app-data-privacy> (May 25, 2016).

Thorin Klosowski, "How mobile phones became a privacy battleground—and how to protect yourself," *New York Times*, <https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones> (September 29, 2022).

Konrad Kollnig, et al., "Before and after GDPR: Tracking in mobile apps," *Internet Policy Review* 10, no. 4, <https://policyreview.info/articles/analysis/and-after-gdpr-tracking-mobile-apps> (December 21, 2021).

Konrad Kollnig, et al., "Goodbye tracking? Impact of iOS app tracking transparency and privacy labels," FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency, <https://dl.acm.org/doi/abs/10.1145/3531146.3533116> (June 2022).

Konrad Kollnig and Nigel Shadbolt, "TrackerControl: Transparency and choice around app tracking," *Journal of Open Source Software* 7, no. 75, <https://www.theoj.org/joss-papers/joss.04270/10.21105.joss.04270.pdf> (July 8, 2022).

Hannah Norman and Victoria Knight, "Should you worry about data from your period-tracking app being used against you?" Kaiser Health Network, <https://khn.org/news/article/period-tracking-apps-data-privacy> (May 13, 2022).

Diana Paiva, "Study shows how much personal data popular mobile gaming apps collect," *Irish Tech News*, <https://irishtechnews.ie/study-personal-data-popular-mobile-gaming-apps> (June 17, 2022).

Semi Park, et al., "Data privacy in wearable IoT devices: Anonymization and deanonymization," *Security and Communication Networks* 2021, article 4973404, <https://www.hindawi.com/journals/scn/2021/4973404> (2021).

Theresa Power, Denes Blazer and Joanne Shepard, "Federal court: September 2022," *LSJ Online* <https://lsj.com.au/articles/federal-court-september-2022> (September 2, 2022).

Aliya Ram, et al., "How smartphone apps track users and share data," *Financial Times*, <https://www.ft.com/products?location=https%3A%2F%2Fmobile-app-data-trackers%2F> (October 22, 2018).

Brian Reed, "Mobile application security: 2021's breaches," *Dark Reading*, <https://www.darkreading.com/application-security/mobile-application-security-2021-s-breaches> (January 4, 2022).

Hailey Reissman, "Americans don't understand what companies can do with their personal data — and that's a problem," Annenberg School for Communication, University of Pennsylvania, <https://www.asc.upenn.edu/news-events/news/americans-dont-understand-what-companies-can-do-their-personal-data-and-thats-problem> (February 7, 2023).

Erdoğan Yağız Şahin, "When your phone gets sick: FluBot abuses Accessibility features to steal data," Security Research Labs, <https://www.srlabs.de/bites/flubot-abuses-accessibility-features-to-steal-data> (December 21, 2021).

Tom Spring, "1,300 popular Android apps access data without proper permissions," *Threat Post*, <https://threatpost.com/apps-access-data-without-permissions/146325> (July 9, 2019).

Surfshark, "Dangers of mobile gaming in the UK," <https://surfshark.com/research/cybersecurity-for-kids/statistics-uk> (December 9, 2020).

Jennifer Valentino-Devries, et al., "Your apps know where you were last night, and can't keep a secret," *New York Times*, <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> (December 10, 2018).

Zhaohua Wang, et al., "Exploring the eastern frontier: A first look at mobile app tracking in China," International Conference on Passive and Active Network Measurement 2020, https://link.springer.com/chapter/10.1007/978-3-030-44081-7_19 (March 18, 2020).

Lauren E. Willis, "Deception by design," *Harvard Journal of Law and Technology* 34, no. 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694575 (2020).

Xueling Zhang, et al., "How does misconfiguration of analytic services compromise mobile privacy?" International Conference on Software Engineering, Seoul, South Korea, <https://galadriel.cs.utsa.edu/~rslavin/publications/icse20.pdf> (June 27-July 19, 2020).